(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2003－510713
（P2003－510713A）
(43)公表日　平成15年３月18日(2003.3.18)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)	
G06F	15/00	330	G06F	15/00	330C	5B058
	1/00			17/60	142	5B076
	17/60	142	G06K	17/00	D	5B085
G06K	17/00				L	5C053
			H04N	7/16	C	5C064

審査請求　未請求　予備審査請求　有　（全 71 頁）　最終頁に続く

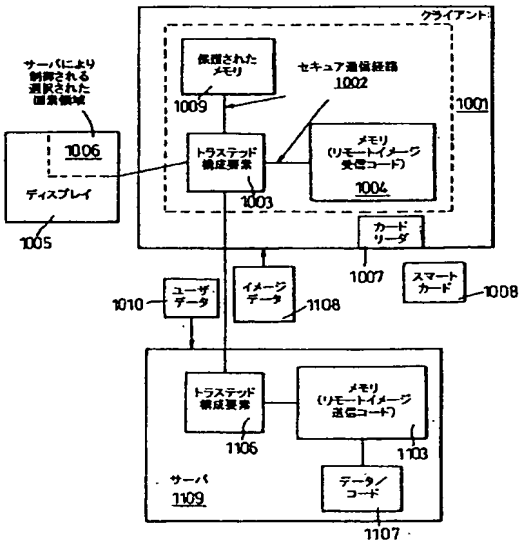
(21)出願番号　特願2001－526683(P2001－526683)
(86)(22)出願日　平成12年９月25日(2000.9.25)
(85)翻訳文提出日　平成14年３月25日(2002.3.25)
(86)国際出願番号　ＰＣＴ／ＧＢ００／０３６８９
(87)国際公開番号　ＷＯ０１／０２３９８０
(87)国際公開日　平成13年４月５日(2001.4.5)
(31)優先権主張番号　９９２２６６５．６
(32)優先日　平成11年９月25日(1999.9.25)
(33)優先権主張国　イギリス（ＧＢ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＪＰ，ＵＳ

(71)出願人　ヒューレット・パッカード・カンパニー
ＨＥＷＬＥＴＴ－ＰＡＣＫＡＲＤ　ＣＯＭＰＡＮＹ
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(72)発明者　ピアソン，シアニ
イギリス国ブリストル・ビーエス９・３ピーゼット，ウエストバーリー－オン－トリム，サンディリーズ・35
(74)代理人　弁理士　古谷　馨　（外３名）

最終頁に続く

(54)【発明の名称】　データの使用を制限するトラステッドコンピューティングプラットフォーム

(57)【要約】
ｸﾗｲｱﾝﾄ/ｻｰﾊﾞｼｽﾃﾑはｻｰﾊﾞ1109により提供されるﾃﾞｰﾀの制限的な使用を提供するよう構成されるｸﾗｲｱﾝﾄﾌﾟﾗｯﾄﾌｫｰﾑ1001を有する。ｸﾗｲｱﾝﾄﾌﾟﾗｯﾄﾌｫｰﾑ1001は、ﾃﾞｨｽﾌﾟﾚｲ1005とｾｷｭｱな通信手段と該ｾｷｭｱな通信手段によりｻｰﾊﾞ1109からﾃﾞｰﾀを受信しかつ該ﾃﾞｰﾀを表示するｲﾒｰｼﾞ受信ｺｰﾄﾞ1004を含むﾒﾓﾘとを備える。ｸﾗｲｱﾝﾄﾌﾟﾗｯﾄﾌｫｰﾑ1001は、ｻｰﾊﾞ1109から受信したﾃﾞｰﾀが非認可の目的ではなく該ﾃﾞｰﾀの表示のために使用されるよう構成される。ﾃﾞｰﾀをｸﾗｲｱﾝﾄﾌﾟﾗｯﾄﾌｫｰﾑに提供して、ｸﾗｲｱﾝﾄﾌﾟﾗｯﾄﾌｫｰﾑにより制限的な使用を行うよう構成されるｻｰﾊﾞ1109は、ｻｰﾊﾞ1109上で実行されるﾃﾞｰﾀのｲﾒｰｼﾞを提供するｲﾒｰｼﾞ送信ｺｰﾄﾞ1103を含むﾒﾓﾘと、ｸﾗｲｱﾝﾄﾌﾟﾗｯﾄﾌｫｰﾑ1001に対するﾃﾞｰﾀのｲﾒｰｼﾞのｾｷｭｱな通信を行うｾｷｭｱな通信手段とを備える。ｻｰﾊﾞ1109は、ｸﾗｲｱﾝﾄﾌﾟﾗｯﾄﾌｫｰﾑ1001がﾃﾞｰﾀの制限的な使用をｲﾒｰｼﾞ送信ｺｰﾄﾞ1103によりﾃﾞｰﾀが送信される前に確実に行うよう構成されることを判定するよう構成される。



イメージ伝送システムの論理図

【特許請求の範囲】

【請求項１】

サーバにより提供されるデータの制限的な使用を提供するよう構成されたクライアントプラットフォームであって、

ディスプレイと、

セキュアな通信手段と、

該セキュアな通信手段によりサーバからデータを受信して該データを表示するためのイメージ受信コードを含むメモリとを備えており、

該クライアントプラットフォームが、サーバから受信した前記データを非認可の目的のためではなく該データの表示のために使用するよう構成されている、クライアントプラットフォーム。

【請求項２】

修正から物理的及び論理的に保護されるクライアントトラステッド構成要素を含み、該クライアントトラステッド構成要素が、サーバから受信したデータが非認可の目的のために使用されることを防止するよう構成されている、請求項１に記載のクライアントプラットフォーム。

【請求項３】

前記クライアントトラステッド構成要素が、該クライアントプラットフォーム上で動作するコードの完全性の基準を提供するよう構成された完全性監視手段を含み、該完全性監視手段が、前記イメージ受信コードの完全性を監視するよう構成される、請求項２に記載のクライアントプラットフォーム。

【請求項４】

前記イメージ受信コードが、前記クライアントトラステッド構成要素内に配設される、請求項２に記載のクライアントプラットフォーム。

【請求項５】

該クライアントプラットフォームのディスプレイが前記クライアントトラステッド構成要素の内部から制御されるように該クライアントトラステッド構成要素内にディスプレイコントローラが配設される、請求項２に記載のクライアントプラットフォーム。

【請求項６】

該クライアントプラットフォームが、前記クライアントトラステッド構成要素に対する直接的なユーザ入力を提供するセキュアなユーザインタフェイスを備えており、前記イメージ受信コードが、前記セキュアなユーザインタフェイスから受信したユーザ入力をサーバへ提供するよう構成される、請求項２ないし請求項５の何れか一項に記載のクライアントプラットフォーム。

【請求項７】

前記クライアントトラステッド構成要素が、他の信頼できる構成要素又はセキュアなトークンを認証するよう構成される、請求項２ないし請求項６の何れか一項に記載のクライアントプラットフォーム。

【請求項８】

前記クライアントトラステッド構成要素が、他のプラットフォームの信頼できる状況を判定するよう構成される、請求項２ないし請求項７の何れか一項に記載のクライアントプラットフォーム。

【請求項９】

ユーザのセキュアなトークンを含むスマートカードを受容するためのスマートカードリーダを更に備えている、請求項１ないし請求項８の何れか一項に記載のクライアントプラットフォーム。

【請求項１０】

前記ディスプレイの一部が、前記クライアントプラットフォームによる如何なる要求にも関わりなく前記サーバにより決定されたデータを表示するために確保される、請求項１ないし請求項９の何れか一項に記載のクライアントプラットフォーム。

【請求項１１】

クライアントプラットフォームによるデータの制限的な使用のために該クライアントプラットフォームにデータを提供するよう構成されたサーバであって、

該サーバ上で実行されるデータのイメージを提供するためのイメージ送信コードを含むメモリと、

前記クライアントプラットフォームに対するデータのイメージのセキュアな通

信を行うためのセキュアな通信手段とを備えており、

前記イメージ送信コードによりデータが送信される前に、前記クライアントプラットフォームが前記データの制限的な使用を確実に行うよう構成されていることを判定するように構成される、サーバ。

【請求項１２】

修正から物理的及び論理的に保護されるサーバトラステッド構成要素を含み、該サーバトラステッド構成要素が、前記クライアントプラットフォーム上で動作するコードの完全性の基準を提供するよう構成された完全性監視手段を含む、請求項１１に記載のサーバ。

【請求項１３】

前記サーバトラステッド構成要素が、他の信頼できる構成要素及びセキュアなトークンを認証するよう構成される、請求項１２に記載のサーバ。

【請求項１４】

イメージデータをユーザにセキュアに提供して制限的な使用を行うシステムであって、

請求項１ないし請求項１０の何れか一項に記載のクライアントプラットフォームと、

請求項１１ないし請求項１３の何れか一項に記載のサーバと

を備えており、前記クライアントプラットフォームのユーザが、前記サーバからのイメージデータを該クライアントプラットフォームにおいて見ることを要求する、システム。

【請求項１５】

ユーザが、前記クライアントプラットフォームにおいて見られるイメージデータを提供するよう前記クライアントプラットフォーム上でのコードの実行を要求する、請求項１４に記載のシステム。

【請求項１６】

ユーザがコードの実行を要求し、該コードが前記クライアントプラットフォーム上で部分的に実行すると共に前記サーバ上で部分的に実行して、前記クライアントプラットフォームにおいて見られるイメージデータを提供し、該イメージ

データが、前記クライアントプラットフォーム上で実行されたコードの結果に関連して該クライアントプラットフォームにおいて見られる、請求項１４に記載のシステム。

【請求項１７】

ユーザスマートカードを更に備えており、該ユーザスマートカードが前記クライアントプラットフォームへの前記イメージデータの送信を可能にするものであることを判定するよう前記サーバが構成される、請求項９に依存する請求項１４ないし請求項１６の何れか一項に記載のシステム。

【請求項１８】

イメージデータをクライアントプラットフォームに提供して制限的な使用を行う方法であって、

クライアントプラットフォームがサーバからのイメージデータを要求し、

該クライアントプラットフォームが、イメージデータを受信する許可を有していると共に該イメージデータを前記制限的な使用のためだけに使用するよう構成されることを、前記サーバが判定し、

セキュアな通信チャネルを介して前記イメージデータを提供する、

という各ステップを含む方法。

【請求項１９】

前記クライアントプラットフォームから前記サーバへ要求データを提供し、該要求データに基づき修正されたイメージデータを提供する、という各ステップを更に含む、請求項１８に記載の方法。

【請求項２０】

前記要求データを提供するステップ及び前記修正されたイメージデータを提供するステップが、必要に応じて多数回繰り返される、請求項１９に記載の方法。

【請求項２１】

イメージデータ又は修正されたイメージデータが前記クライアントプラットフォームに提供された後に使用ログを更新するステップを更に含む、請求項１８ないし請求項２０の何れか一項に記載の方法。

【請求項２２】

許可を判定する前記ステップが、ユーザ許可を含むスマートカードが前記クライアントプラットフォームとセッション中であるか否かを判定することを含む、請求項１８ないし請求項２１の何れか一項に記載の方法。

【請求項２３】

前記イメージデータの一部が、前記クライアントプラットフォームからの何れの要求とも関わりなく前記サーバによって決定される、請求項１８ないし請求項２２の何れか一項に記載の方法。

【請求項２４】

前記イメージデータの一部が広告コンテンツを含む、請求項２３に記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、クライアント／サーバシステムにおいて信頼できる端末機能を提供すること、及びコンテンツ又はソフトウェアが誤用されるリスクを該コンテンツ又はソフトウェアの所有者に与えることなくユーザに対するコンテンツの提供又はユーザによるソフトウェアの試用を提供することに関する。

【０００２】

【従来の技術】

本明細書において、「データ」は、イメージ、ソフトウェア、及びストリーミングメディアといったディジタル的に作成することが可能なあらゆるものを表す。

【０００３】

将来には、コンピュータシステムは、よりセキュアな起動を実現すると共に、他のコードに対する完全性チェックを行ってウイルスその他による未認証の修正がオペレーティングシステム及び実装されているソフトウェアに対して行われていないことを確実にすることが可能になるであろう。更に、次世代のタンパーブルーフ（改ざん防止）装置が、既に市場に現れており、又はまもなく現れると思われるものがあり、これらは、外部又は携帯モジュール（スマートカード等）と内部モジュール（セキュリティ機能を有する埋め込み式プロセッサ、半埋め込み式プロセッサ、又はコプロセッサ、すなわち、マザーボード、ＵＳＢ（ユニバーサルシリアルバス）及びＩＳＡ（業界標準アーキテクチャ）機器を含む）との両方を含むものである。これらのタンパーブルーフモジュールを使用してシステムのハードウェアが改ざんされていないかチェックし、これにより、現在入手可能なもの（例えばイーサネット名）よりも信頼できる形のマシン識別(identity)が提供されることになる。

【０００４】

【発明が解決しようとする課題】

これにもかかわらず、データの著作権侵害や、ソフトウェア開発者とエンドユ

ーザとの両者にとって許容可能な態様でのソフトウェアのライセンス制(licensing)又は従量制(metering)での使用に関する対策は、依然として重大な問題となっている。

【0005】

ソフトウェアライセンシングは、ハッキングや著作権侵害にさらされており、現在使用されているソフトウェアライセンシング法の全てはそれらに関連する問題を有している。ライセンシングのソフトウェアによる実施（ライセンス管理システム等）は柔軟性のあるものではあるが、格別安全でも高速でもない。特に、これらは、セキュリティの欠如（例えば一般的な「ハッキング」を受け易い）及びソフトウェアの真正な交換(genuine replacement)の困難性といった問題を有している。逆に、ハードウェアによる実施（ドングル）は、ソフトウェアによる実施に比べて高速であり一般により安全であるが柔軟性に欠けるものである。これは、特定の個々のソフトウェアに専用設計されるものであるため、エンドユーザにとっては不便なものとなる。

【0006】

コンテンツ保護の分野における従来技術として、コンテンツのウォーターマーキング、コンテンツを囲むソフトウェアラッパー、パスワード保護、及び指紋技術といった技術が挙げられる。更に、クライアントマシンに送信されるコンテンツの暗号化や、クライアントマシンに送信されてコンテンツを復号できるようにする復号鍵を含む、様々なアプローチが存在する。これらのアプローチは全て、潜在的な欠点を有するものであり、すなわち、クライアントマシンが信頼できないものである可能性があり、また、データが復号され又は他の方法で（例えば、保護機構のハッキング若しくはクリアバージョン(clear version)のコピーにより）クライアントマシンにとって使用可能になった際に、該データが誤用される可能性がある。

【0007】

【課題を解決するための手段】

本発明の第１の態様では、サーバにより提供されるデータの制限を伴った使用を提供するよう構成されたクライアントプラットフォームが提供される。該クラ

イアントプラットフォームは、ディスプレイと、セキュアな通信手段と、該セキュアな通信手段によりサーバからデータを受信して該データを表示するためのイメージ受信コードを含むメモリとを備えており、未認証の目的ではなくデータの表示を目的として、サーバから受信したデータを使用するように構成される。

【０００８】

本発明の第２の態様では、クライアントプラットフォームによる制限を伴ったデータの使用のために該クライアントプラットフォームにデータを提供するよう構成されたサーバが提供される。該サーバは、該サーバ上で実行されたデータのイメージを提供するためのイメージ送信コードを含むメモリと、クライアントプラットフォームに対するデータのイメージのセキュアな通信のためのセキュアな通信手段とを備えており、これにより、前記イメージ送信コードによりデータが送信される前に該データの制限を伴った使用が確実になるようクライアントプラットフォームが構成されていることを判定するよう該サーバが構成される。

【０００９】

本発明の第３の態様では、イメージデータをその制限を伴った使用のためにユーザにセキュアに提供するシステムが提供される。該システムは、上述のクライアントプラットフォームと上述のサーバとを備えたものであり、該クライアントプラットフォームのユーザは、該サーバからのイメージデータを該クライアントプラットフォームにおいて見ることを要求する。

【００１０】

本発明の第４の態様では、イメージデータをその制限を伴った使用のためにクライアントプラットフォームに提供する方法が提供される。該方法は、該クライアントプラットフォームが、サーバからのイメージデータを要求し、該サーバが、該クライアントプラットフォームが該イメージデータを受信する許可を有していると共に制限を伴った使用のためだけに該イメージデータを使用するよう構成されていることを判定し、セキュアな通信チャネルを介して該イメージデータを提供する、という各ステップを含むものである。

【００１１】

本発明の好適な実施形態は、全機能を有する(full function)プラットフォー

ムにおいて強化された信頼できる端末機能を提供するものとなる。これにより、リモートで処理されたデータを表示すると共に該データの誤用を防止することが可能となる。本システムは、個人情報の保護、データのライセンシング、又は複製又は誤用のリスクを伴うことなく試用版ソフトウェアに全機能を持たせるといった、広範なサービスに使用することができるため、クライアント、サーバ、又は開発者に利益をもたらすものとなる。かかる利益が得られるのは、データ自体を複製又は修正することができないようにデータを忠実に出力するものであると該クライアントプラットフォームを信頼することができるからである。このため、例えば、試用ソフトウェアで全機能を使用することが可能であるが、これはセキュリティの危険性を伴うため、現時点では稀なケースである。エンドユーザにも利点があり、その１つとして、電子メールメッセージといった機密情報(sensitive information)をクライアントマシンのハードディスクに格納する必要がなくなるため、ホットデスキング(hot desking)状況（公共の場での共有端末の使用等）においてかかる情報の秘匿性(confidentiality)又は完全性に対する攻撃から該情報を効果的に保護することができることが挙げられる。

【００１２】

コンテンツ保護に対する本発明の複数の実施形態におけるアプローチは、既存の従来技術のモデルとは異なり、本発明の場合には、情報の少なくとも一部が、耐改ざん性（tamper-resistant）のハードウェアの内部にある保護されたメモリ、又は該耐改ざん性のハードウェアによってのみアクセス可能な保護されたメモリに一般に一時的に記憶された後に削除され、該部分はハードディスクには格納されない。該耐改ざん性ハードウェアは、認証のために、イメージの出力を制御するために、そして随意選択的に課金のために使用される。クライアントマシンは、上述した従来のモデルの場合のようにデータパッケージ全体（保護されていても保護されていなくても良い）を取得することが決してないため、従来のアプローチが被りやすい態様でクライアントマシンを介してソフトウェアを誤用することが不可能となる。このため、例えば、ユーザは、画面をコピーしたり、又は画面からテキストをリタイプすることは可能であるが、オリジナルドキュメントをコピーすることはできず、また音楽の場合には、ユーザは、サウンドトラック

を聴き、その音を部屋で録音することは可能であるが、そのディジタルオブジェクトを直接コピーすることはできないことになる。これは、著作権侵害の興味を顕著に削ぐものとなる。

【００１３】

本発明の実施形態は、データのコピー及び未認証での使用からの保護、並びにペイ・パー・ユーズ(pay-per-use：従量制／使った分だけ支払う方式)及び時間依存モデル(time-dependent model)といったライセンシングモデルの柔軟性の増大という利点に加えて、クライアントプラットフォームに格納されているデータラッパーの修正又は削除といったハッキングの試行からの保護を提供するものとなる。これは、かかる格納が本モデルでは決して行われず、また、クライアントプラットフォーム内の耐改ざん性ハードウェアが、該プラットフォーム内のあらゆるイメージの改変に対する保護を行うからである。より詳細には、試用の度にユーザにデータアクセスが許可される場合には、現時点では、かかるデータにおける使用制御(usege control)の複製又は修正の危険性が高すぎるため、一層質の低い(inferior)製品しか試用のために送信することができない、と一般に考えられている。本発明の実施形態により提供されるシステムは、完全な機能を有するソフトウェア又は完全な解像度を有するイメージを、エンドユーザが吟味することを可能にする。

【００１４】

本発明の実施形態によるシステムは、ソフトウェアライセンシング、又は上述の完全な機能を有する試用ソフトウェアの提供を目的として使用することが可能であるが、該目的の代わりに、又は該目的に加えて、クライアントの個人情報を保護するために試用することが可能である。例えば、エンドユーザが耐改ざん性ハードウェアを内蔵する共有端末にログインして（場合によってはリモートログインを使用して）個人情報にアクセスする場合には、該情報は、ハードディスク上ではなく、該耐改ざん性ハードウェアの内部にあり又は該耐改ざん性ハードウェアでしかアクセスできない保護されたメモリのみに記憶され、ユーザがログアウトした後には完全に削除することができる。

【００１５】

本発明の好適な実施形態では、クライアントプラットフォーム（及びサーバ）は、タンパープルーフ構成要素（又は「トラステッド(trusted：信頼できる)モジュール」）を、好ましくは該タンパープルーフ構成要素内で実行しているソフトウェアと共に使用する。該ソフトウェアは、かかるコンピュータプラットフォーム間で転送されるデータイメージの操作及び該データイメージに関する選択を制御するものである。１つ又は複数の該トラステッドモジュールは、トラステッド端末機能が完全な機能を有するプラットフォームにおいて提供されることを確実にする際に重要な役割を果たすものである。従量記録(metering record)をタンパープルーフ装置又はスマートカードに記憶し、必要に応じて再び管理者に報告することが可能である。データに関する登録及び支払いを可能にするための関連するクリアリングハウス機構が存在することも可能である。

［００１６］

トラステッドモジュール又は構成要素は好適には、内部データの未認証の修正又は検査に対する免疫性を有するものとなる。該トラステッドモジュールは、偽造(forgery)を防止するための物理的なものであり、模造(counterfeiting)を防止するための耐改ざん性を有し、好適には距離をおいたセキュアな通信を行うための暗号機能を有するものとなる。トラステッドモジュールの構築方法は、本質的に当業者に周知のところである。トラステッドモジュールは、暗号方法を使用して、該モジュール自体に暗号的な識別（cryptographic identity）を提供し、及び真正性(authenticity)、完全性(integrity)、秘匿性(confidentiality)を提供し、リプレイ攻撃(replay attack)から保護し、ディジタル署名を行い、必要に応じてディジタル証明書を使用することが可能である。上述その他の暗号方法及びその初期設定については、セキュリティに関わる当業者に周知のところである。

［００１７］

特に好適な構成では、本発明の実施形態を採用したライセンシングシステムは、セキュアな通信経路により互いに接続された少なくとも２台のコンピュータプラットフォーム（１台がサーバとして、もう１台がクライアントとして機能する）から構成される。各コンピュータプラットフォームは、内部的な改ざんに耐性

を有すると共に第三者の公開鍵証明書を格納するトラステッドモジュールと、リモートイメージングコード（サーバの場合には、該サーバ上で実行するデータのイメージに対応する情報をサーバから他のトラステッド（信頼できる）プラットフォームに送信するためのインタフェイスを提供するリモートイメージングコードであり、クライアントの場合には、クライアントプラットフォームのモニタに表示することが可能なデータのイメージに対応する情報を他のトラステッドプラットフォームから受信するため及び／又はかかるイメージの実行に関連するユーザ選択を捕捉しこれを中継してサーバプラットフォームに返すためのインタフェイスを提供するリモートイメージ受信コード）を格納する手段と、第三者の秘密鍵を用いて署名されたリモートイメージングコードをハッシュしたバージョン（変形したもの）を格納する手段とを有しており、該コンピュータプラットフォームは、該プラットフォームの起動時にリモートイメージングコードの完全性を前記署名されたバージョン及び公開鍵証明書を参照してチェックし、該完全性チェックに失敗した場合にリモートイメージングコードのロードを阻止するようプログラムされる。この完全性チェックに失敗した場合に、プラットフォームの全ての完全性が失敗するように構成することが可能である。随意選択的に、リモートイメージングコードの機能の一部を、ソフトウェアではなくローカルのトラステッド構成要素内のハードウェアにより実行することが可能である。１つ又は２つ以上のスマートカードは、それに関連するリーダと共に、コンピュータプラットフォームの追加の随意選択的な構成要素であり、該スマートカードは、（プラットフォームではなく）ユーザライセンスを提供してイメージデータへのアクセスを可能とするものである。

【００１８】

トラステッド端末機能は、多数の異なる方法で使用されることが可能である。極端な形態の一般的なモデルは、ライセンスを受けたデータをクライアントではなくサーバ上で実行することである。支払いと引き替えに、クライアントは、トラステッドサーバ上でのデータの実行に対応するイメージング情報を受信する。これは、サーバ上のリモートイメージ送信コードを介して送信される。その後、クライアントマシン上のリモートイメージ受信コードが、ユーザの選択に対応す

るキーボードストロークをサーバに送信し、次いでアプリケーションの実行の変化に対応するイメージング情報を受信する。該イメージング情報は、トラステッドサーバからＰＰＴＰといったセキュアなチャネルを介してクライアント内のトラステッド構成要素に直接送信される。該トラステッド構成要素は、コンピューティング装置のアントラステッド（信頼できない）構成要素を全く伴わずにイメージング情報を直接表示するよう構成されたものである。

【００１９】

実際に如何なる量のソフトウェアをクライアント上で実行するかに関して得ることができる他の見込みが存在する。全てのソフトウェアをクライアントではなくサーバ上で実行することは、全ての場合において効率的ではない。比較的機密性の高い情報の場合（これはデータアクセスに該当し、又はソフトウェアが実行する度に実質的な重複が存在し得る場合）、全てのイメージをクライアントの保護されたメモリに一時的に格納して、ソフトウェア（実際にはサーバ上で実行されているもの）をクライアント上に表示させるのが適切である。クライアントは、保護されたメモリに格納されているイメージとは別にソフトウェアを格納する段階がないため、ハードディスクその他の記憶媒体を介したデータのライセンス侵害攻撃を受けにくい。機密性のより低い情報の場合、特に、ゲームソフトウェアの場合に普通であるようにアプリケーションがその実行の度に異なるイメージを生成する可能性がある場合には、ソフトウェアの一部のみをサーバで実行するのがおそらく一層適切であり、例えば、実質的にローカルでソフトウェアが実行されるが、該ソフトウェアを実行するために（オンラインサービスといった）サーバからの所定の重要な入力が必要となる、といった具合である。サーバは、依然として全体的な制御を掌握している必要があるため、クライアントマシンがプログラムを実行できる場合であっても、サーバの介在なしでかかる実行を成功させることはできない。これを実行する様々な方法が存在し、例えば、サーバは、情報のキービットを供給し、全てのクライアントにとって同一となる共同ブロック(communal block)でイメージを送信し、クライアントのトラステッド構成要素が、サーバのトラステッド構成要素に対して個人情報又はキービットの認証を繰り返し行うことが可能であり、又は、データの一部をローカルに格納し、サーバ

が追加データを保護されたメモリに送信することが可能である。効率化のために、実行中又は実行後に、情報の一部（キービット等）のみを保護されたメモリに格納し、残りの情報をハードディスクその他の記憶媒体に格納することが可能である。このイメージ転送の部分的なモデル(partial model)は、同一サーバ上の異なるデータに関する全体的なモデル(total model)と同時に使用することが可能である。

【００２０】

サーバは、トラステッド環境にあり、データ又はラッパーの改変又は複製から保護されている。したがって、ペイ・パー・ユーズ及び時間依存モデルといったライセンシングモデル並びにより伝統的なモデルをセキュアな態様で使用することが可能である。

【００２１】

好適には、表示処理は、ユーザに対する表示を破壊する(subvert)ことができないようにトラステッド構成要素内から制御される。ユーザのスマートカードがイメージデータを入手する必要がある場合には、リーダに挿入されたスマートカードの所有者のみがその正しい印章イメージであることを知っている印章イメージをクライアントのディスプレイに表示して、クライアントとサーバとの接続のセキュリティをチェックすることができる。課金情報の提供といった機密性のあるタスクをスマートカードの所有者が実行する前に、スマートカードは、クライアントプラットフォームのトラステッド構成要素からの認証を必要とすることが可能であり（この認証はクライアントモニタに印章イメージを表示することにより強化することが可能である）、このため、あらゆる機密情報の伝送前にスマートカードの所有者からの許可を必要とすることが可能である。

【００２２】

随意選択的に、トラステッドクライアントプラットフォームにおける選択された画素領域の表示を、（おそらくは第三者の代わりに）サーバのトラステッドプラットフォームにより代替的に使用するために確保することができる。この所定の画素領域は、時間と共に変動することが可能であり、トラステッドサーバプラットフォーム上で実行されているデータと直接関係がないと思われる情報を伝送

することも可能である。これにより、サーバのトラステッドプラットフォーム又は信頼できる第三者により送信された表示イメージ中に、広告又は他の所有権を有する情報を組み込むことが可能となる。

【００２３】

【発明の実施の形態】

次に、本発明の一実施形態を実例を介して説明する。この好適な実施形態のシステムの一部が、トラステッド構成要素を含む（後述する）クライアントプラットフォームであり、該トラステッド構成要素は、ユーザ、又は該クライアントプラットフォームと通信している他者が該クライアントプラットフォームとセキュアで信頼できる対話を行うことを可能にする。かかるトラステッド構成要素については、以下で説明するが、「Trusted Computing Platform」と題する2000年2月15日付けで出願された本出願人の同時係属中の国際特許出願第PCT/GB00/00528号でより完全に説明されている。該クライアントプラットフォーム内のトラステッド構成要素はまた、クライアントプラットフォームのディスプレイを制御して、ディスプレイ上に表示されたものが、クライアントプラットフォーム上で動作している非認可プロセスによって破壊されていないことを、ユーザが確信できるようにする。本実施形態のトラステッド構成要素についても後述するが、「System for Digitally Signing a Document」と題する2000年5月25日付けで出願された本出願人の同時係属中の国際特許出願第PCT/GB00/01996号でより完全に説明されている。本システムはまた、好適な実施形態においてユーザの個人的なトラステッドトークンを使用する。該トラステッドトークンは、本書で詳述する一実施形態ではユーザスマートカードである。更に、本書で解説する実施形態では、クライアントプラットフォームだけでなくサーバもまたトラステッド構成要素を含むものとなる（但し、この場合にはトラステッド（信頼できる）表示機能を有している必要がある）。

【００２４】

本システムの特定の構成要素、すなわち、トラステッド表示機能を含むトラステッド構成要素及びユーザスマートカードについて、図１ないし図９を参照して詳述する。本発明において、トラステッドコンピューティングプラットフォーム

（及びトラステッド構成要素）、トラステッドディスプレイ、及びスマートカードの特定の形態は重要ではなく、特許請求の範囲から逸脱することなく変更することが可能である、ということが当業者には理解されよう。

【００２５】

トラステッドコンピューティングプラットフォームを達成するために、物理的なトラステッドデバイスがコンピューティングプラットフォームに組み込まれる。該トラステッドデバイスは、プラットフォームの完全性に関する基準(integrity metric)を提供する信頼性の尺度となる(reliably measured)データにプラットフォームの識別を結びつける機能を有するものである。該トラステッドデバイスは、（後述するように）トラステッド表示プロセッサとして機能することも可能である。

【００２６】

トラステッド表示プロセッサ（又はそれと同様の特性を有するデバイス）は、標準的なホストコンピュータソフトウェアによりデータを操作できるポイントを越えたビデオ処理の一段階でビデオデータと関連するものである。これにより、トラステッド表示プロセッサは、ホストコンピュータソフトウェアによる干渉又は破壊を受けることなく、データをディスプレイ画面上に表示することが可能となる。このため、トラステッド表示プロセッサは、ユーザに対して如何なるイメージが現在表示されているかを確認することができる。識別及び完全性に関する基準は、プラットフォームの信頼性を保証する用意のある信頼できる第三者（ＴＰ：trusted party）により提供された期待値と比較される。それらが一致する場合、これは、完全性基準の範囲に依存してプラットフォームの少なくとも一部が正常に動作していることを意味する。

【００２７】

ユーザは、プラットフォームの正常な動作を確認した後、該プラットフォームと他のデータをやり取りする。ユーザは、トラステッドデバイスの識別及び完全性の基準を提供するよう該トラステッドデバイスに要求することにより該確認を行う（随意選択的に、トラステッドデバイスは、それ自体がプラットフォームの正常な動作を確認できなかった場合に、識別の証明(evidence)の提供を拒否する

ことが可能である）。ユーザは、識別及び完全性の基準の証拠(proof)を受け取り、該証拠を正しいと確信している値と比較する。該正しい値は、ＴＰ、又はユーザが信頼している別のエンティティ(entity)により提供される。トラステッドデバイスにより報告されたデータがＴＰにより提供されたものと同一である場合、ユーザは該プラットフォームを信頼することになる。これは、ユーザが該エンティティを信頼しているからである。該エンティティが該プラットフォームを信頼しているのは、該エンティティが以前に該プラットフォームの識別の正当性を立証する(validate)と共にその完全性基準が正しいと判定したからである。

【００２８】

ユーザは、プラットフォームのトラステッド動作を確立すると、他のデータをプラットフォームと交換する。ローカルユーザの場合、該交換は、該プラットフォーム上で動作しているソフトウェアアプリケーションとの対話により行うことが可能である。またリモートユーザの場合には、該交換は、セキュアなトランザクションを伴う可能性がある。いずれの場合であっても、交換されたデータは、トラステッドデバイスにより「署名」される。これにより、ユーザは、信頼できる挙動を有するプラットフォームとの間でデータが交換されている、という一層大きな確信を持つことができる。

【００２９】

トラステッドデバイスは、暗号プロセスを使用するが、必ずしもこれらの暗号プロセスに対する外部的なインタフェイスを提供する必要はない。また、ほとんどの望ましい実施形態は、トラステッドデバイスをタンパーブルーフにし、該トラステッドデバイスが他のプラットフォーム機能にアクセスできないようにすることにより秘密を保護し、及び権限なき修正に対して十分な免疫性を有する環境を提供するものとなる。タンパーブルーフは不可能であるため、最も近いものは、耐改ざん性を有する又は改ざんを検出するトラステッドデバイスである。このため、トラステッドデバイスは、耐改ざん性を有する物理的な構成要素からなることが好ましい。

【００３０】

耐改ざん性に関する技術は、セキュリティ分野における当業者には周知のとこ

ろである。かかる技術として、改ざんに抗する方法（トラステッドデバイスの適当なカプセル化等）、改ざんを検出する方法（仕様外の電圧、Ｘ線、又はトラステッドデバイス筐体内における物理的な完全性の損失の検出等）、及び改ざんの検出時におけるデータの除去方法が挙げられる。適当な技術に関する更なる説明については、http://www.cl.cam.ac.uk/~mgk25/tamper.htmlに見られる。タンパープルーフは、本発明の最も望ましい特徴であるが、本発明の通常動作に含まれるものではなく、このため本発明の範囲を超えているため、本明細書では詳述しないこととする。

【００３１】

トラステッドデバイスは、物理的なものであることが好ましい。これは、トラステッドデバイスが、偽造(forge)の困難なものでなければならないからである。最も好ましくは、トラステッドデバイスは、耐改ざん性を有するものとなる。これは、トラステッドデバイスが、模造(counterfeit)が困難なものでなければならないからである。トラステッドデバイスは典型的には、暗号プロセスを使用することが可能なエンジンを有するものとなる。これは、ローカル又はリモートで識別を証明する必要があるからであり、トラステッドデバイスはまた、関連することになるプラットフォームの完全性基準を測定する少なくとも１つの方法を含むものとなる。

【００３２】

図１は、ホストコンピュータシステムを示している。この場合、ホストコンピュータは、（例えば）WindowsNT(TM)オペレーティングシステムの元で動作するパーソナルコンピュータすなわちＰＣである。図１によれば、ホストコンピュータ100は、視覚表示装置（ＶＤＵ）105、キーボード110、マウス115、スマートカードリーダ120、及びローカルエリアネットワーク（ＬＡＮ）125に接続され、該ＬＡＮ125がインターネット130に接続される。ここで、スマートカードリーダは、独立したユニットであるが、キーボードの一体部分とすることも可能である。ＶＤＵ、キーボード、マウス、及びトラステッドスイッチは、ホストコンピュータのヒューマン／コンピュータインタフェイス（ＨＣＩ）と考えることができる。より具体的には、ディスプレイは、信頼できるコントロールの下で動作する場合には、

後述するように「トラステッドユーザインタフェイス」の一部として考えることができる。図１はまた、後述するように本実施形態において使用されるスマートカード122を示している。

【００３３】

図２は、図１のホストコンピュータのハードウェア構成を示す。

【００３４】

図２によれば、ホストコンピュータ100は、中央処理装置(ＣＰＵ)200すなわちメインプロセッサが、ＲＡＭ205及びＲＯＭ210からなる主メモリに接続され、これらは全てホストコンピュータ100のマザーボード215上に実装されている。この場合のＣＰＵはPentium™プロセッサである。該ＣＰＵは、ＰＣＩ (Peripheral Component Interconnect) ブリッジ220を介してＰＣＩバス225に接続され、該ＰＣＩバスにホストコンピュータ100の他の主要な構成要素が接続される。該ＰＣＩバス225は、適当なコントロール、アドレス及びデータ部分からなるが、ここでは詳述しないこととする。Pentium™プロセッサ及びＰＣＩアーキテクチャに関する本記載の範囲を超える詳細については、Hans-Peter Messmer著の書籍「The Indispensable PC Hardware Handbook」（第3版、Addison-Wesley出版、ISBN0-201-40399-4)を参照されたい。勿論、本実施形態は、Pentium™プロセッサ、Windows™オペレーティングシステム、又はＰＣＩバスを使用した実施に限定されるものではない。

【００３５】

ＰＣＩバス225に装着されるホストコンピュータ100の他の主要な構成要素として、ＳＣＳＩ(small computer system interface)バス235を介してハードディスクドライブ2600及びCD－ROMドライブ2605に接続されるＳＣＳＩアダプタ、ホストコンピュータ100をＬＡＮ（local area network）125に接続すると共に該ＬＡＮ125を介してホストコンピュータ100がファイルサーバ、プリントサーバ、又は電子メールサーバ等の他のホストコンピュータ（図示せず）及びインターネット130と通信することを可能にするＬＡＮアダプタ250、キーボード110、マウス115、及びスマートカードリーダ120を装着するためのＩＯ（入出力）デバイス225、及びトラステッドデバイス260（トラステッド表示プロセッサ機能を組み込んだ

もの）が挙げられる。該トラステッド表示プロセッサは、全ての標準的な表示機能に加えて多数の更なるタスクを扱うものである。これについて以下で詳述する。「標準的な表示機能」とは、任意の標準的なホストコンピュータ100（例えば、WindowsNT(R)オペレーティングシステムの下で動作しているＰＣ）においてオペレーティングシステム又はアプリケーションソフトウェアに関連したイメージを表示する場合に見られることが通常期待される機能である。

【００３６】

全ての主要な構成要素（特にトラステッドデバイス260）は、ホストコンピュータ100のマザーボード215に一体化されることが好ましいが、場合によっては、ＬＡＮアダプタ250及びＳＣＳＩアダプタ230をプラグインタイプのものとすることが可能である。

【００３７】

通常、パーソナルコンピュータにおいて、ＢＩＯＳプログラムは、特別に予約されたメモリ領域215、すなわち、システムメモリの最初の1メガバイトの上位64K（アドレスF000h～FFFFh）にあり、メインプロセッサは、業界全体の標準にしたがって最初にこのメモリロケーションを参照するよう構成される。

【００３８】

本プラットフォームと従来のプラットフォームとの大きな違いは、リセット後に、メインプロセッサが最初にトラステッドデバイスにより制御され、次いでプラットフォームに固有のＢＩＯＳプログラムに制御が渡され、次いで全ての入出力デバイスが通常通りに初期化される点である。ＢＩＯＳプログラムの実行後には、ＢＩＯＳプログラムによって通常通りにWindowsNT（TM）等のオペレーティングシステムプログラムに制御が渡され、該オペレーティングシステムプログラムが典型的にはハードディスクドライブから主メモリへとロードされる。

【００３９】

明らかに、通常の手順からの該変更は、業界標準の実施に修正を加えることを必要とし、該修正により、メインプロセッサ200は、トラステッド構成要素（トラステッドデバイスとも記載する）260にアドレス指定を行ってその最初の命令を受信するよう命令されることになる。この変更は、単に異なるアドレスをメイ

ンプロセッサ200にハードコード化(hard-coding)することにより実施することが可能である。代替的には、トラステッドデバイス260に標準的なＢＩＯＳプログラムアドレスを割り当てることも可能であり、この場合には、メインプロセッサの構成を修正する必要がなくなる。

【００４０】

ＢＩＯＳブートブロックをトラステッドデバイス260内に包含させることが非常に望ましい。これにより、完全性基準を取得する際の破壊（不正なソフトウェアプロセスが存在する場合にも発生し得る）が防止されると共に、ＢＩＯＳが（それ自体が正しい場合であっても）オペレーティングシステムの適正な環境を構築することができなくなる状況を不正なソフトウェアプロセスが生成することが防止される。

【００４１】

本書で説明する好適な形態では、トラステッドデバイス260は、単一の独立した構成要素であるが、代替的にトラステッドデバイス260の機能を、マザーボード上の多数のデバイスへと分離すること、又はプラットフォームの既存の標準的なデバイスのうちの１つ又は２つ以上に一体化することが予想される。例えば、トラステッドデバイスの機能の１つ又は２つ以上をメインプロセッサ自体に一体化することは、上記機能及びその通信が破壊され得ない場合には実施可能である。しかし、これは、トラステッド機能によってのみ使用される別個のリード線がプロセッサ上に必要になる可能性がある。該実施形態に加えて、又は該実施形態の代わりに、本実施形態ではトラステッドデバイスはマザーボード215と一体化させるよう構成されたハードウェアデバイスであるが、トラステッドデバイスは、必要に応じてプラットフォームに装着されるドングルといった「リムーバブル」デバイスとして実施可能であることが考えられる。トラステッドデバイスを一体化させるか又は取り外し可能とするかは設計上の選択事項である。しかし、トラステッドデバイスを分離可能とする場合には、トラステッドデバイスとプラットフォームとの間の論理的な結合を提供する機構が存在する必要がある。

【００４２】

システムのリセット後に、トラステッドデバイス260は、セキュアブートプロ

セスを実行して、プラットフォーム100のオペレーティングシステム（システムクロック及びモニタ上の表示を含む）が正常かつセキュアな態様で動作していることを確実にする。該セキュアブートプロセスにおいて、トラステッドデバイス260は、コンピューティングプラットフォーム100の完全性基準を取得する。該トラステッドデバイス260はまた、セキュアなデータ転送、及び、例えば該デバイス260とスマートカードとの間での暗号／復号及び署名／検証を介した認証を実行することができる。トラステッドデバイス260はまた、ユーザインタフェイスのロックといった様々なセキュリティ制御ポリシーをセキュアに強化することが可能である。更に、本構成では、トラステッドデバイス260は、トラステッド表示プロセッサとしても作用し、これにより、表示プロセッサの標準的な表示機能と共に、トラステッドユーザインタフェイスを提供するための特別な非標準的な機能も提供する。

【００４３】

図３によれば、トラステッドデバイス260は、

コントローラ300と、

該マイクロコントローラ300の動作を制御するための個々の制御プログラム命令（すなわちファームウェア）を含むフラッシュメモリ等の不揮発性メモリ305であって、該制御プログラムが、完全性基準をコンピューティングプラットフォームから取得する測定機能370と、スマートカード（又は他のトラステッド構成要素）の認証を行う認証機能380とを含む、不揮発性メモリ305（代替的にはトラステッドデバイス260はＡＳＩＣで実施することが可能であるが、ＡＳＩＣは一般に大量生産ではより優れた性能及びコスト効率を提供するが一般に開発コストが高く柔軟性に劣るものとなる）と、

トラステッドデバイス260をＰＣＩバスに接続し、イメージデータ（すなわちグラフィクスプリミティブ）を含む情報をＣＰＵ200から受信すると共に後述するように信頼できるイメージデータをスマートカード122から受信するための、インタフェイス310と、

少なくとも１つの完全なイメージフレームを格納するための十分なＶＲＡＭ（ビデオＲＡＭ）を備えたフレームバッファメモリ315（典型的なフレームバッフ

ァメモリ315のサイズは１～２Mbyteであり、この場合の画面解像度は最大1,670万色をサポートする1280×768となる）と、

ピクスマップ(pixmap)データをアナログ信号に変換するビデオＤＡＣ（ディジタルアナログ変換器）320であって、ビデオインタフェイス325を介して該ビデオＤＡＣ320に接続している（アナログ）ＶＤＵ105を駆動する、ビデオＤＡＣ320と、

状況情報、特に受信した暗号鍵を格納し、及びマイクロコントローラ300に作業領域を提供する、揮発性メモリ335（例えばＤＲＡＭ（ダイナミックＲＡＭ）又はより高価なＳＲＡＭ（スタティックＲＡＭ）と、

ハードウェア暗号アクセラレータ及び／又はソフトウェアを含む暗号プロセッサ340であって、トラステッドデバイス260に暗号識別を提供し、及び以下で詳述するように、真正性、完全性、及び秘匿性を提供し、リプレイ攻撃からの保護を提供し、ディジタル署名を行い、及びディジタル証明書を使用するように構成された、暗号プロセッサ340と、

トラステッドデバイス260の識別子$I_{D,P}$（例えば、単純なテキストストリング名。これは、トラステッドデバイスに関連するデータのインデックス及びラベルに使用可能であるが、それ自体は、トラステッド状況下でプラットフォームの識別を証明するには不十分なものである）、トラステッドデバイス260の秘密鍵$S_{D,P}$、及びVerSign Inc.といった信頼できる第三者認証機関(certification agency)（ＴＰ）により署名され提供された証明書$Cert_{D,P}$であって、トラステッドデバイス260を、署名(signature)公開鍵－秘密鍵対及び機密(confidentiality)公開鍵－秘密鍵対と結びつけ、及びトラステッドデバイス260の対応する公開鍵を含む、証明書$Cert_{D,P}$を格納する、不揮発性メモリ345（例えばフラッシュメモリ）とを備えたものとなる。

【００４４】

証明書は典型的には、上記情報を含むが、ＣＡの公開鍵は含まない。該公開鍵は典型的には、「公開鍵インフラストラクチャ（ＰＫＩ）」を使用して入手することが可能である。ＰＫＩの動作は、セキュリティ技術に関する当業者には周知のものである。

【００４５】

証明書$Cert_{p,p}$は、トラステッドデバイス260の公開鍵を第三者に提供するために使用される。これは、第三者が該公開鍵の出所を確信すると共に該公開鍵が有効な公開－秘密鍵対の一部であることを確信するよう行われる。このように、第三者がトラステッドデバイス260の公開鍵を事前に知っていること又はこれを取得することは必要ない。

【００４６】

証明書$Cert_{p,p}$（又は随意選択的な更に別の証明書）は、トラステッドデバイス260の公開鍵だけでなく、信頼できる第三者（ＴＰ）により判定されたプラットフォームの完全性基準の認証された値も含む。後の通信セッションにおいて、プラットフォーム100のユーザは、取得した完全性基準を証明書における認証された完全性基準と比較することにより、プラットフォーム100の完全性を検証することができる。それらの値が一致した場合、ユーザは、プラットフォーム10が破壊されていないことを確信することができる。ＴＰの一般的に入手可能な公開鍵を知ることにより、証明書の単純な検証が可能となる。

【００４７】

トラステッドデバイス260には、該デバイスが関係するコンピューティングプラットフォーム100の完全性基準を確実に測定し又は取得する少なくとも１つの方法が搭載されている。本実施形態では、完全性基準は、ＢＩＯＳメモリ中のＢＩＯＳ命令のダイジェストを生成することにより測定機能370により取得される。かかる取得された完全性基準は、上述のように検証された場合に、プラットフォーム100がハードウェアレベル又はＢＩＯＳプログラムレベルで破壊されていないという一層高いレベルの信頼性(confidence)をプラットフォーム100の潜在的なユーザに与えるものとなる。典型的には、他の周知のプロセス（例えばウイルスチェッカ）が適所に配設されてオペレーティングシステム及びアプリケーションプログラムコードが破壊されていないことをチェックすることになる。

【００４８】

測定機能370は、ハッシュプログラム390及びトラステッドデバイス260の秘密鍵$S_{p,p}$を格納する不揮発性メモリ305,345、並びに取得された完全性基準をダイジ

エスト361という形で格納する揮発性メモリ335に対するアクセスを有するものである。適当な実施形態では、揮発性メモリ335を使用して、プラットフォーム100に対するアクセスを得るために使用することができる１つ又は２つ以上の真正なスマートカード122の公開鍵及び関連するIDラベル360a～360nを格納することも可能である。

【００４９】

一好適実施形態では、ダイジェストと同様に、完全性基準がブール値を含み、該ブール値が測定機能370により揮発性メモリ335に格納される。この理由は後に明らかとなろう。

【００５０】

次に、完全性基準を取得する好適なプロセスについて図４を参照して説明する。

【００５１】

ステップ500において、スイッチONで、測定機能370がＰＣＩバス225上のメインプロセッサ200の活動を監視して、アクセスされた最初のメモリがトラステッドデバイス260があるか否かを判定する。従来の動作では、メインプロセッサは、ＢＩＯＳプログラムを実行するためにまずＢＩＯＳメモリに向かう。しかし、図示の構成によれば、メインプロセッサ200は、メモリとして作用するトラステッドデバイス260に向かう。ステップ505で、アクセスされた最初のメモリがトラステッドデバイス260である場合には、ステップ510で、測定機能370は、アクセスされた最初のメモリがトラステッドデバイス260であったことを示すブール値を揮発性メモリ335に書き込む。それ以外の場合には、ステップ515で、アクセスされた最初のメモリがトラステッドデバイス260でなかったことを示すブール値を書き込む。

【００５２】

勿論、アクセスされた最初のメモリがトラステッドデバイス260でない場合には、トラステッドデバイス260が全くアクセスされない可能性がある。これは、例えば、最初にＢＩＯＳプログラムを実行させるようメインプロセッサ200が操作された場合に該当する。かかる状況では、プラットフォームは動作するが、そ

の完全性をオンデマンドで検証することができない。これは、完全性基準を入手できないことになるからである。更に、ＢＩＯＳプログラムがアクセスされた後にトラステッドデバイス260がアクセスされた場合には、ブール値は、明らかにプラットフォームの完全性の欠如を示すものとなる。

【００５３】

ステップ520で、メインプロセッサ200によりメモリとしてアクセスされたとき（又はアクセスされた場合には）、メインプロセッサ200は、ステップ525で測定機能370から格納されている元のハッシュ命令390を読み出す。該ハッシュ命令390がメインプロセッサ200により処理するためにデータバス225を介して渡される。ステップ530において、メインプロセッサ200は、該ハッシュ命令390を実行し、ステップ535においてこれらを使用して、ＢＩＯＳメモリ215のコンテンツ（内容）を読み出し、及び該コンテンツをハッシュプログラムに従って処理することにより、ＢＩＯＳメモリ215のダイジェストを計算する。ステップ540において、メインプロセッサ200が、該計算されたダイジェスト361をトラステッドデバイス260の適当な不揮発性メモリロケーション335に書き込む。次いでステップ545において、測定機能370が、ＢＩＯＳメモリ215中のＢＩＯＳプログラムを呼び出して、従来の態様で実行を続行する。

【００５４】

必要とされる信頼の範囲に応じて完全性基準を計算することが可能な多数の異なる方法が存在することは明らかである。ＢＩＯＳプログラムの完全性の測定は、プラットフォームの根底にある処理環境の完全性についての基本的なチェックを提供する。該完全性基準は、ブートプロセスの妥当性についての推論を可能にする（すなわち、該完全性基準の値を使用してプラットフォームが正しいＢＩＯＳを使用して起動されたか否かを確認することができる）形であるべきである。随意選択的に、ＢＩＯＳ内の個々の機能ブロックは、独自のダイジェスト値を有することが可能であり、全体のＢＩＯＳダイジェストは、これら個々のダイジェストのダイジェストである。これにより、意図する目的にとってＢＩＯＳ動作のどの部分が重大であるか及びどの部分が無関係であるかを特定するポリシーが可能となる（この場合には、該ポリシー下で動作の妥当性を確立することができる

ように個々のダイジェストを格納しなければならない）。

【００５５】

他の完全性チェックとして、プラットフォームに装着された様々な他のデバイス、構成要素、又は装置が存在すると共に、かつ正しい動作順(working order)になっていることを確立することが挙げられる。一例では、ＳＣＳＩコントローラに関連するＢＩＯＳプログラムを検証して、周辺機器との通信を確実に信頼できるものにすることが可能である。別の例では、プラットフォーム上の他のデバイス（例えばメモリデバイス又はコプロセッサ）の完全性を、固定のチャレンジ／レスポンス(challenge/response)対話を実施して一貫した結果を保証することにより検証することができる。トラステッドデバイス260が分離可能な構成要素である場合には、かかる何らかの形態の対話が、トラステッドデバイス260とプラットフォームとの間の適当な論理的結合を提供することが望ましい。また、トラステッドデバイス260は、本実施形態ではプラットフォームの他の部品と通信する主要な手段としてデータバスを使用しているが、有線経路又は光学経路等の代替的な通信経路を提供するよう実施することが可能であり、かかる構成を図８及び図９を参照して更に詳述する。更に、本実施形態では、トラステッドデバイス260は、完全性基準を計算するようメインプロセッサ200に命令するが、他の実施形態では、トラステッドデバイス自体が１つ又は２つ以上の完全性基準を測定するように構成される。

【００５６】

好適には、ＢＩＯＳブートプロセスは、ブートプロセス自体の完全性を検証するための機構を含む。かかる機構は、例えばIntel社の草案「Wired for Management baseline specification v 2.0 - Boot Integrity Service)」からすでに周知であり、ソフトウェア又はファームウェアをロードする前に該ソフトウェア又はファームウェアのダイジェストを計算することを含む。かかる計算されたダイジェストは、信頼できるエンティティ（その公開鍵はＢＩＯＳにとって既知である）により提供された証明書に格納されている値と比較される。次いで、計算された値が証明書から期待される値と一致し、及び該信頼できるエンティティの公開鍵を使用することにより証明書が有効であることが証明された場合にのみ、ソ

フトウェア／ファームウェアがロードされる。それ以外の場合には、適当な例外処理ルーチンが呼び出される。

【００５７】

随意選択的に、計算されたＢＩＯＳダイジェストを受信した後、トラステッドデバイス260は、証明書におけるＢＩＯＳダイジェストの正しい値を調べ、計算されたダイジェストが該正しい値と一致しない場合にはＢＩＯＳに制御を渡さないようにすることができる。これに加えて、又は代替的に、トラステッドデバイス260は、ブール値を調べ、アクセスされた最初のメモリがトラステッドデバイス260でなかった場合には制御をＢＩＯＳに戻さないようにすることができる。これらのいずれの場合にも、適当な例外処理ルーチンを呼び出すことができる。

【００５８】

図５は、ＴＰ、プラットフォームに組み込まれるトラステッドデバイス260、及びトラステッドプラットフォームの完全性を検証することを望む（リモートプラットフォームの）ユーザによる動作フローを示している。ユーザがローカルユーザである場合にも、図５に示すものと実質的に同一のステップが呼び出されることが理解されよう。いずれの場合にも、ユーザは典型的には、検証確認を実施するために、何らかの形のソフトウェアアプリケーションに依存することになる。該ソフトウェアアプリケーションをリモートプラットフォーム又はトラステッドプラットフォーム上で動作させることは可能である。しかし、リモートプラットフォーム上であっても、何らかの方法でソフトウェアアプリケーションが破壊される可能性がある。したがって、高レベルの完全性のためには、ソフトウェアアプリケーションは、検証を目的として適当なリーダに挿入されることになるユーザのスマートカード上に存在することになると考えられる。図５は、一般的な場合の動作の流れを示しており、ユーザのスマートカードによる検証動作のより具体的な流れについては図６を参照して更に後述する。

【００５９】

第１の例では、トラステッドプラットフォームを保証するＴＰは、プラットフォームの種類を調べてその保証をするか否かを判定する。これは、ポリシー上の問題である。全てが良好であれば、ステップ600において、ＴＰは、プラットフ

ォームの完全性基準の値を測定する。次いで、ＴＰは、ステップ605においてプラットフォームの証明書を生成する。該証明書は、トラステッドデバイスの公開鍵（及び随意選択的にそのIDラベル）を、測定された完全性基準に追加し、及び該ストリングにＴＰの秘密鍵を署名することにより、ＴＰにより生成される。

【００６０】

次いで、トラステッドデバイス260は、該秘密鍵を使用して、ユーザから受信した入力データを処理して出力データを生成することにより、その識別を検証することができる。この場合、該入出力対は、秘密鍵を知らなければ生成することが統計的に不可能なものである。このため、秘密鍵に関する知識は、この場合の識別の基本を形成するものとなる。対称暗号を使用して識別の基本を形成することが実施可能であることは明らかである。しかし、対称暗号を使用する欠点は、ユーザが該ユーザ自身の秘密をトラステッドデバイスと共有する必要があることにある。更に、秘密をユーザと共有する必要がある結果として、対称暗号は基本的にユーザに対する識別を証明するには十分であるが、トラステッドデバイス又はユーザから発信された検証を完全に確信することができない第三者に対して識別を証明するには不十分なものとなる。

【００６１】

ステップ610において、トラステッドデバイス260は、トラステッドデバイス260の適当な不揮発性メモリロケーションに証明書を書き込むことにより初期化される。これは、好適には、マザーボード215へのインストール後のトラステッドデバイス260との間のセキュアな通信によって行う。トラステッドデバイス260への証明書の書き込み方法は、スマートカードに秘密鍵を書き込むことにより該スマートカードを初期化する際に使用される方法と同様である。セキュアな通信は、トラステッドデバイス（又はスマートカード）に対してその製造時に書き込まれる「マスタキー」（ＴＰしか知らないもの）によってサポートされる。該マスタキーは、トラステッドデバイス260に対するデータの書き込みを可能にするために使用され、該マスタキーを知らなければトラステッドデバイス260に対するデータの書き込みは不可能となる。

【００６２】

プラットフォームの動作時の後の時点、例えば、プラットフォームがスイッチONXはリセットされた場合に、ステップ615において、トラステッドデバイス260は、プラットフォームの完全性基準を取得して格納する。

【００６３】

ユーザは、プラットフォームとの通信を行いたい場合には、ステップ620において、乱数等のナンス(nonce)を作成し、ステップ625において、トラステッドデバイス260にチャレンジを行う（プラットフォームのオペレーティングシステム、又は適当なソフトウェアアプリケーションは、このチャレンジを認識し、これを典型的にはＢＩＯＳタイプのコールを介してトラステッドデバイス260に適当な態様で渡すよう構成される）。ナンスは、信頼できないプラットフォームによる古いが真正の署名のリプレイによって引き起こされるなりすまし(deception)（リプレイ攻撃と呼ばれる）からユーザを保護するために使用される。該ナンスを提供しレスポンスを検証するプロセスは、周知の「チャレンジ／レスポンス」プロセスの一例である。

【００６４】

ステップ630において、トラステッドデバイス260は、チャレンジを受信して、適当なリプレーを作成する。これは、測定された完全性基準及びナンスのダイジェスト並びに随意選択的にそのIDラベルとすることが可能である。次いでステップ635において、トラステッドデバイス260は、その秘密鍵を使用して前記ダイジェストに署名し、該署名したダイジェストを証明書$Cert_{P,}$と共にユーザに返送する。

【００６５】

ステップ640において、ユーザは、該チャレンジレスポンスを受信し、ＴＰの周知の公開鍵を使用して証明書を検証する。次いでユーザは、ステップ650において、トラステッドデバイス260の公開鍵を証明書から抽出し、該公開鍵を使用して、署名されたダイジェストをチャレンジレスポンスから復号する。次いでステップ660において、ユーザは、チャレンジレスポンス中のナンスを検証する。次いでステップ670において、ユーザは、計算された（チャレンジレスポンスから抽出した）完全性基準を、証明書から抽出した正しいプラットフォーム完全性

基準と比較する。ステップ645,655,665,又は675において、上記の検証ステップのいずれかに失敗した場合には、ステップ680において全ての処理が終了し、これ以上の通信は行われない。

【００６６】

全て成功したものと仮定すると、ステップ685,690において、ユーザ及びトラステッドプラットフォームが、他のプロトコルを使用して、他のデータについてのセキュアな通信を確立し、好適には該プラットフォームからのデータがトラステッドデバイス260により署名される。

【００６７】

この検証プロセスを更に洗練させることが可能である。チャレンジャが、チャレンジを介して、プラットフォーム完全性基準の値と、これを入手した方法との両方に理解していることが望ましい。これらの部分的な情報は共に、プラットフォームの完全性についての正しい判定をチャレンジャに行わせるものであることが望ましい。また、チャレンジャは、多数の異なるオプションも使用可能であり、すなわち、トラステッドデバイス260において完全性基準が有効であると識別されることを許容することが可能であり、また代替的に、完全性基準の値がチャレンジャにより保持される値と等しい場合にのみ、プラットフォームが関連するレベルの完全性を有することを許容することが可能である（又は、これら２つの場合に異なるレベルの信頼があると考えることも可能である）。

【００６８】

署名、証明書の使用、及びチャレンジ／レスポンス、並びにこれらを使用した識別の証明といった技術は、セキュリティ技術に関する当業者に周知のものであるため、本書ではこれ以上詳述する必要はない。

【００６９】

本システムの好適な構成において、ユーザは、スマートカード122を使用してトラステッドプラットフォームを検証する。この好適な実施形態に従った使用に適したスマートカードの処理エンジンを図７に示す。該処理エンジンは、標準的な暗号及び復号機能を実施して他の場所から受信した情報の検証をサポートするプロセッサ400を備える。本実施形態において、プロセッサ400は、８ビットマイ

クロコントローラであり、組み込みオペレーティングシステムを有しており、及びISO 7816-3, 4, T=0, T=1, T=14の各規格により指定される非同期プロトコルを介して外界と通信するよう構成されている。スマートカードはまた、不揮発性メモリ420（例えばフラッシュメモリ）から構成され、スマートカード122の識別子I_{sc}、データのデジタル署名に使用される秘密鍵S_{sc}、及び信頼できる第三者認証機関により提供された証明書$Cert_{sc}$（スマートカードを公開－秘密鍵対と結びつけ、及びスマートカード122の対応する公開鍵を含むもの－本質的にはトラステッドデバイス260の証明書$Cert_{pp}$と同一）を収容する。更に、該スマートカードは、詳細を後述する、プロセスがユーザのスマートカードにより安全に動作していることをユーザに示すためにトラステッド表示プロセッサ260によりグラフィカルに表すことができる「印章」データSEALを不揮発性メモリ420に含む。本実施形態では、印章データSEALは、ユーザにより一意の識別子（例えばユーザ自身のイメージ）として当初に選択されて周知の技術によりスマートカード122にロードされるピクスマップイメージという形のものである。プロセッサ400は、状況情報（受信した鍵等）を格納し、及びプロセッサ400に作業領域を提供する、揮発性メモリ430（例えばＲＡＭ）と、スマートカードリーダと通信するためのインタフェイス440（例えば電気接点）とのアクセスも有する。

【００７０】

印章イメージは、ピクスマップとして格納される場合には比較的大量のメモリを消費し得る。これは、メモリ容量が比較的制限されるスマートカード122にイメージが格納される必要がある状況において明らかに不利となる可能性がある。メモリ要件は、多数の異なる技術によって低減できる。例えば、印章イメージは、トラステッドデバイス260により解凍可能な圧縮イメージと、トラステッドデバイス260により生成されるモザイクの繰り返しのプリミティブ要素を形成するサムネイルイメージと、トラステッドデバイス260により単一の大きなイメージとして表示することが可能であり又は上述のサムネイルイメージとして使用することができる自然圧縮(naturally compressed)イメージ（例えば一組の英数字キャラクタ）とを含むことが可能である。これら代替例のいずれにおいても、印章データ自体は暗号化形式とし、その表示を行う前に該データを復号するためにト

ラステッドデバイス260が必要となるようにすることが可能である。代替的に、印章データは、ホストコンピュータ100又はネットワークサーバにより格納された多数の考え得るイメージのうちの１つを識別する暗号化されたインデックスとすることが可能である。この場合には、該インデックスがセキュアなチャネルを介してトラステッドデバイス260によりフェッチされ復号され、これにより、正しいイメージを読み出して表示することが可能となる。更に、印章データは、適当にプログラムされたトラステッドデバイス260により解釈されてイメージを生成することが可能な命令（例えばPostScript™命令）から構成することが可能である。

【００７１】

上述のように、図６は、ユーザがスマートカード122を用いてトラステッドプラットフォームと対話することによりプラットフォームの完全性を検証する実例の動作フローを示している。後述するように、本プロセスは、チャレンジ／レスポンスルーチンを有利に実施する。多数の使用可能なチャレンジ／レスポンス機構が存在する。本実施形態において使用される認証プロトコルの実施形態は、ISO/IEC9798-3「Information technology - Security techniques - Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm)」（国際標準化機構、11月 12293)に記載されるような相互（又は３ステップ）認証である。勿論、例えば、同参考文献に記載されているような２ステップ又は４ステップといった他の認証手順を使用できない理由はない。

【００７２】

まず、ユーザは、ステップ700において、プラットフォームのスマートカードリーダ120に自分のスマートカード122を挿入する。

【００７３】

予め、このようにユーザによって使用されるよう構成されたプラットフォームは、典型的には、標準的なオペレーティングシステムの制御下で動作し、認証プロセスを実行するものであり、ユーザが自分のスマートカード122を挿入するまで待機する。このようにしてスマートカードリーダ120がアクティブになっている場合を除き、該プラットフォームは、典型的には、ユーザインタフェイス（す

なわち、画面、キーボード、及びマウス）を「ロック」することにより、ユーザに対してアクセス不能な状態にされる。

【００７４】

スマートカード122がスマートカードリーダ120に挿入されると、トラステッドデバイス260がトリガされて、ステップ705でナンスAを生成してスマートカード122に送信することにより、同期をとって(in step)相互認証を試行する。乱数等のナンスは、信頼できない第三者による古いが真正のレスポンスのリプレイ（「リプレイ攻撃」と呼ばれる）により引き起こされるなりすまし(deception)から発信者を保護するために使用される。

【００７５】

これに応じて、ステップ710において、スマートカード122が、ナンスA、スマートカード122により生成された新たなナンスB、トラステッドデバイス260のID、及び幾つかの冗長の平文と、スマートカード122の秘密鍵を使用して該平文に署名することにより生成される平文の署名と、スマートカード122のIDと公開鍵とを含む証明書との連結(concatenation)を含むレスポンスを生成して返送する。

【００７６】

トラステッドデバイス260は、ステップ715において、証明書中の公開鍵を使用して平文の署名を検証することによりレスポンスの認証を行う。レスポンスが真正(authentic)でない場合には、本プロセスはステップ720において終了する。またレスポンスが真正である場合には、ステップ725において、トラステッドデバイス260が、ナンスA、ナンスB、スマートカード122のID、及び取得した完全性基準の平文と、トラステッドデバイス260の秘密鍵を使用して該平文に署名することにより生成される平文の書名と、トラステッドデバイス260の公開鍵と真正な完全性基準と（双方ともＴＰの秘密鍵により署名されたもの）を備えた証明書との連結を含む更なるレスポンスを生成して送信する。

【００７７】

スマートカード122は、ステップ730において、ＴＰの公開鍵を使用し、及び取得した完全性基準を真正な完全性基準と比較することにより、前記レスポンスの

認証を行う。この場合の一致は検証の成功を示すものとなる。該更なるレスポンスが真正でない場合には、本プロセスはステップ735において終了する。

【００７８】

該手順が成功した場合には、トラステッドデバイス260がスマートカード122の認証を完了すると共に、スマートカード122がトラステッドプラットフォームの完全性の検証を完了し、ステップ740において、認証プロセスがユーザのセキュアなプロセスを実行する。

【００７９】

特定のタイプの対話では、この時点で認証プロセスが終了することができる。しかし、ユーザとトラステッドプラットフォームの間でセッションが続行されるべき場合には、該ユーザがプラットフォームに対して認証された状態を維持することを確実にすることが望ましい。

【００８０】

継続した認証が必要とされる場合には、本認証プロセスは、ステップ745においてインターバルタイマを設定する。その後、本認証プロセスは、適当なオペレーティングシステムの割り込みルーチンを使用してインターバルタイマを周期的に作動(service)させて、ステップ750において、該タイマが所定のタイムアウト時間に到達し又はこれを越えたときを検出する。

【００８１】

明らかに、本認証プロセス及びインターバルタイマは、セキュアなプロセスと並行して動作するものである。タイムアウト時間に到達し又はこれを超過した場合には、本認証プロセスは、ステップ760において、トラステッドデバイス260をトリガしてスマートカード122の再認証を行わせる。該再認証は、ステップ760において、スマートカード122の身元を確認するためのチャレンジを該スマートカード122へ送信することにより行われる。スマートカード122は、ステップ765において、そのID及びその公開鍵を含む証明書を返送する。ステップ770において、（例えばスマートカード122が取り外されている結果として）レスポンスがない場合、又は何らかの理由により証明書が有効でなくなっている場合（例えばスマートカードが別のスマートカードと交換された場合）には、ステップ775にお

いて、トラステッドデバイス260により本セッションが終了される。ステップ770において、それ以外の場合には、インターバルタイマをリセットすることによりステップ745からのプロセスを繰り返す。

【００８２】

実施形態によっては、上記に加えて、又は上記の代替策として、ユーザプロフィールを暗号化し署名してプライバシー及び完全性を保護する必要がある。かかる場合には、トラステッドデバイス260とスマートカード122との間にセキュアなデータ転送プロトコルが必要となる可能性がある。セキュアなクレデンシャル(credential)を２つのエンティティ間で転送する多数の使用可能な機構が存在する。本実施形態において使用することが可能な考え得る実施形態は、ISO/IEC DIS 11770-3「Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques」（ＩＳＯ、1997年3月）からの安全鍵転送機構(secure key transport mechanisms)である。

【００８３】

他の周知のチャレンジ／レスポンス技法を使用した検証プロセスの変形例は、当業者により容易に実施可能なものである。同様に、異なる態様で（すなわち、スマートカードを備えたユーザとしてでなく）プラットフォームと対話する複数のユーザが複数の代替的な検証プロセスを使用することが可能である。

【００８４】

上述のように、トラステッドデバイス260は、その識別及びトラステッドプロセスをホストコンピュータに提供し、トラステッド表示プロセッサは、その耐改ざん性、偽造(forgery)に対する耐性、及び模造(counterfeiting)に対する耐性に基づく特性を有する。適当な認証機構を備えた選択されたエンティティのみが、トラステッドデバイス260の内部で動作しているプロセスに作用することが可能である。ホストコンピュータの一般的なあらゆるユーザ、該ホストコンピュータにネットワークを介して接続される一般的なあらゆるユーザ又は一般的なあらゆるエンティティは、トラステッドデバイス260内で動作しているプロセスにアクセスし又は干渉することが不可能となる。トラステッドデバイス260は「侵されていない(inviolate)」という特性を有するものとなる。

【００８５】

フレームバッファメモリ315がＣＰＵ200ではなくトラステッド表示プロセッサ260自体によってのみアクセス可能であることは図３から明らかである。これは本好適な実施形態の重要な特徴である。ＣＰＵ200（又はより重要には破壊的なアプリケーションプログラム又はウイルス）がトラステッド動作中にピクスマップを修正できないことが必要不可欠であるからである。勿論、ＣＰＵ200がフレームバッファメモリ315に直接アクセスすることができる場合であっても、トラステッド表示プロセッサ260が、該ＣＰＵ200がフレームバッファメモリ315にアクセスできるときについて最終的な制御を有するよう構成される限り、同一レベルのセキュリティを提供することが可能である。明らかに、この後者の方式の方が実施が困難なものとなる。

【００８６】

次いで、ホストコンピュータ100によりグラフィクスプリミティブが生成される典型的なプロセスを技術的背景として説明する。まず、特定のイメージを表示しようとするアプリケーションプログラムは、グラフィカルＡＰＩ（アプリケーションプログラミングインタフェイス）を介して適当なコールをオペレーティングシステムに対して行う。ＡＰＩは典型的には、イメージを表示することを目的としてWindowsNT™により提供されるような特定の根本的な表示機能にアクセスするための標準的なインタフェイスをアプリケーションプログラムに提供するものである。ＡＰＩコールにより、オペレーティングシステムに個々のグラフィクスドライバライブラリルーチンコールを行わせ、その結果として、表示プロセッサ（この場合にはトラステッド表示プロセッサ260）に固有のグラフィクスプリミティブが生成される。かかるグラフィクスプリミティブは、最終的にはＣＰＵ200によってトラステッド表示プロセッサ260に渡される。グラフィクスプリミティブの例としては、「ラインを太さｚで点ｘから点ｙまで描く」又は「各点ｗ，ｘ，ｙ，ｚにより囲まれた領域を色ａで塗りつぶす」といったものが挙げられる。

【００８７】

マイクロコントローラ300の制御プログラムは、受信したグラフィクスプリミティブを処理するための標準的な表示機能が提供されるように該マイクロコント

ローラを制御し、詳細には、

グラフィクスプリミティブをＣＰＵ200から受信し処理して、ＶＤＵ105の画面上に表示されるべきイメージを直接表すピクスマップデータを形成し、ここで、該ピクスマップデータが、ＶＤＵ105画面上のアドレス指定可能な各画素の赤、緑、及び青の各ドットの各々毎に強度値を一般に含み、

該ピクスマップデータをフレームバッファメモリ315に格納し、

周期的に（例えば１秒間に６回）フレームバッファメモリ315からピクスマップデータを読み出し、該データをビデオＤＡＣを使用してアナログ信号へと変換し、該アナログ信号をＶＤＵ105に送信して必要なイメージを画面に表示させる、といった制御を行う。

【００８８】

標準的な表示機能と別に、制御プログラムは、ＣＰＵ200からのなりすましの(deceived)表示イメージデータを信頼できるイメージデータと合成して単一のピクスマップを形成する機能を含む。制御プログラムはまた、暗号プロセッサとの対話も管理する。

【００８９】

トラステッド表示プロセッサ260は、ホストコンピュータ100の全体的な「表示システム」の一部を形成し、その他の部分は典型的にはオペレーティングシステムの表示機能である。該オペレーティングシステムの表示機能は、アプリケーションプログラムにより「コール」することが可能なものであり、グラフィクスプロセッサ及びＶＤＵ105の標準的な表示機能にアクセスするものである。換言すれば、ホストコンピュータ100の「表示システム」は、イメージの表示に関するハードウェア又は機能のあらゆる部分から構成されるものである。

【００９０】

次いで図８を参照する。同図は、トラステッド構成要素260が使用するためのトラステッド通信経路が配設された好適な構成を示している。かかる構成については、「Communication between Modules of a Computing Apparatus」と題する、2000年2月15日付けで出願された本出願人の同時係属中の国際特許出願第PCT/GB00/00504号に一層完全に記載されている。図８（同図では図２の各要素の一部

のみが示されている）において、ホストコンピュータ100は、メインＣＰＵ200と、ＳＣＳＩインタフェイス230と、ＰＣＩネットワークインタフェイスカード106と、ＤＲＡＭメモリ205とを有し、それらの間に従来の（通常の）通信経路110（ＩＳＡ、ＥＩＳＡ、ＰＣＩ、ＵＳＢ等）が設けられている。該ネットワークインタフェイスカード106はまた、ホストコンピュータ100の外部の世界との外部通信経路112を更に有している。

【００９１】

ネットワークインタフェイスカード106は、「赤」データ領域114と「黒」データ領域116とに論理的に分割され、該領域間にインタフェイス118が配設される。赤領域114では、通常データは平文であり、検出不能な改変や望ましくない盗聴を受けやすく脆弱である。黒データ領域116では、データは、検出不能な改変や望ましくない盗聴から保護される（好適には標準的な暗号機構により暗号化される）。インタフェイス118は、赤情報が黒領域116に漏出しないようにする。インタフェイス118は、好適には標準的な暗号方法及び電子的な隔離技術を使用して赤及び黒領域114,116を分離する。かかる赤／黒領域114,116及びインタフェイス118の設計及び構造は、セキュリティ及び電子の分野、特に軍事分野の当業者には周知のところである。通常の通信経路110及び外部通信経路112は、ネットワークインタフェイスカード106の黒領域116と接続している。

【００９２】

ホストコンピュータ100はまたトラステッドモジュール260を含み、該トラステッドモジュール260は、通常の通信経路110に対してだけでなく、ＣＰＵ220、ＳＣＳＩインタフェイス230、及びネットワークインタフェイスカード106の赤領域114に対しても、相互に別個の追加の通信経路122（符号122a,122b,122c）により接続される。他の構成も可能であり、かかる専用の通信経路が全ての構成要素に配設されるわけではなく、その一例として、トラステッドモジュール260は、メモリ205に対しては、かかる別個の追加の通信経路122を有していない。

【００９３】

トラステッドモジュール260は、それぞれ追加の通信経路122a,122b,122cを介して、ＣＰＵ102、ＳＣＳＩインタフェイス230、及びネットワークインタフェイ

スカード106の赤領域114と通信することができる。トラステッドモジュール260はまた、通常の通信経路110を介して、ＣＰＵ260、ＳＣＳＩインタフェイス230、ネットワークインタフェイスカード106の黒領域116、及びメモリ205と通信することができる。トラステッドモジュール260はまた、該トラステッドモジュール260に格納されているポリシーの制御下で、該トラステッドモジュール260及び追加の通信経路122を介して、ＣＰＵ200、ＳＣＳＩインタフェイス230、及びネットワークインタフェイスカード106の赤領域114の間で特定の情報をルーティングする100VGスイッチセンタとしても機能することができる。トラステッドモジュール260はまた、暗号鍵を生成して、該暗号鍵を、追加の通信経路122a,122b,122cをそれぞれ介して、ＣＰＵ200、ＳＣＳＩインタフェイス230、及びネットワークインタフェイスカード106の赤領域114に分配することができる。

【００９４】

図９は、トラステッドモジュール260がプラットフォームにおける暗号機能を有する唯一のモジュールである場合に、到来する外部のセキュアなメッセージを処理するプロセスを示している。外部メッセージ146は、外部通信経路112を使用してネットワークインタフェイスカード106の黒領域116により受信される。ネットワークインタフェイスカード106は、何らかのデータ並びに認証及び完全性チェックの要求を含むプロトコルデータユニット148を、通常の通信経路110を使用してトラステッドモジュール260へ送信する。トラステッドモジュール260は、該トラステッドモジュール260の内部にある長期鍵（トラステッドモジュール260の外部には決して露呈しないはずのもの）を使用して認証及び完全性チェックを実行し、「OK」の指示を含むプロトコルデータユニット150を追加の通信経路122cを使用してネットワークインタフェイスカード106の赤領域114に送信する。次いでネットワークインタフェイスカード106は、何らかのデータと復号の要求とを含むプロトコルデータユニット152を通常の通信経路110を使用してトラステッドモジュール260に送信する。トラステッドモジュール260は、該トラステッドモジュール260の内部にある一時鍵又は長期鍵を使用してデータを復号し、該復号されたデータを含むプロトコルデータユニット154を追加の通信経路122aを使用してＣＰＵ200に送信する。次いでＣＰＵが適当な処置を行う。

【００９５】

次いで、本発明の特定の実施形態を実施するシステムについて図１０を参照して説明する。

【００９６】

好適な構成では、ユーザは、スマートカードリーダ1007を介してクライアントのトラステッドプラットフォーム1001に接続するユーザスマートカード1008の支援を伴って、クライアントのトラステッドプラットフォーム1001にログインする。クライアントのトラステッドプラットフォーム、スマートカード、及びその間の対話は、基本的には図１ないし図９に関して上述した通りである（但し、これは本発明の全ての実施形態の実施にとって不可欠なものではない）。したがって、クライアントのトラステッドプラットフォーム内には、表示プロセッサを含むクライアントのトラステッド構成要素1003が存在し、ディスプレイ1005上の出力が該クライアントのトラステッド構成要素により制御され、これにより該出力が信頼できるようになっている。クライアントのトラステッドプラットフォーム1001内にはまた、リモートイメージングコードを含むメモリ領域1004と保護されたメモリ領域1009とが含まれる。これらは、トラステッド用途のために利用可能である必要がある。これらは、トラステッド構成要素1003自体の内部に位置することが理想的であるが、これはトラステッド構成要素の製造コストが高くなる結果となる場合がある（保護されたメモリ1009の一部又は全部をトラステッド構成要素内部に設けることはセキュリティとコストとのバランスである）。図１０に示す潜在的により安価な代替例では、保護されたメモリ1009及びリモートイメージングコード1004は、トラステッド構成要素1003の外部に配置されているが、セキュアな通信経路1102（基本的には図８及び図９に関して説明したように専用の通信リンク、理想的にはハードワイヤードであってクライアントのトラステッドプラットフォーム1001の他のあらゆる構成要素から分離されたもの）により該トラステッド構成要素1003に接続されている。保護されたメモリ1009及びリモートイメージングコード1004が、クライアントのトラステッドプラットフォーム上に配置されており、該クライアントのトラステッドプラットフォームの構成要素のうちトラステッド構成要素1003以外のあらゆる構成要素にアクセスできるようにな

っている場合には、例えば「Data Integrity Monitoring in Trusted Computing Entity」と題する、2000年5月25日付けで出願された本出願人の同時係属中の国際特許出願第PCT/GB00/02003号において記載されるように、少なくともそれらの完全性がクライアントのトラステッド構成要素により監視されることが望ましい。クライアントのトラステッドプラットフォーム1001は、図１に示すような構成要素（ユーザ入力のためのキーボードその他のデバイスを含む）を含むことになるが、これについてはここで更に説明する必要はない。

【００９７】

ディスプレイ1005は、クライアントのトラステッド構成要素1003の制御下で動作する。好適な構成では（以下で更に説明するが）、ディスプレイにおける選択された一領域の画素1006は、本システムがクライアント／サーバモードで動作する場合には、リモートサーバの直接的な制御下で動作するよう構成される。ディスプレイ1005は、データをユーザに提供する唯一の可能な方法ではなく、すなわち、サーバは、イメージデータではなく、オーディオプレーヤ（好適にはディスプレイ1005と同じ方法で破壊から保護されるセキュアなオーディオプレーヤ……なお、オーディオプレーヤの場合には、再生されたコンテンツの再録音が極めて容易であるため、セキュリティの有効性が低くなる）により部分的に再生されることになるオーディオデータ又はビデオデータを提供することが可能であり、又は他の形式の出力を全てユーザに提供することも可能である、ということが理解されよう。本発明を実施する場合には、データの機能的な目的は重要ではなく、権限のない使用からデータを保護することが重要である。

【００９８】

クライアントのトラステッド構成要素1003は、ディスプレイ1005に出力されたイメージが、データの実行に確実に対応するものとなるようにする。クライアントのトラステッド構成要素はまた、サーバのトラステッド構成要素1106（以下参照）の認証にも必要とされる。有利にも、クライアントのトラステッド構成要素はまた、サーバのトラステッド構成要素1106のデータ保護能力を検証するように構成される。クライアントのトラステッド構成要素1003に必要とされる考え得る他の役割は、ユーザスマートカード1008（但しこれが使用される場合）を検証す

ること、及び信頼できる性能関連情報を提供することである。この場合には、該情報の提供が、コードの実行時におけるプラットフォームの信頼性の表示であろうと、コード又はデータの実行に関する信頼できる測定(metering)であろうと、報告の提供又は課金情報の提供が行われる。

【００９９】

サーバ1109は、本構成では、図１ないし図９を参照して説明した種類のトラステッドプラットフォームでもある（但し、トラステッド表示機能はおそらく必要なく、他の構成も明らかに実施可能である）。該サーバ1109は、サーバのトラステッド構成要素1106と、リモートイメージ送信コード1103を含むメモリ領域と、アプリケーションデータ1107を格納するためのメモリとを含む。この場合も、特に、リモートイメージ送信コード1103は、サーバのトラステッド構成要素1106内に、又は使用されるクライアントのトラステッド構成要素1103を参照して説明した複数の代替的な構成のうちの１つ内に存在することができる。

【０１００】

サーバのトラステッド構成要素1106は、利用形態に応じて、クライアントのトラステッド構成要素1003、ユーザスマートカード1008、又はその両者を認証することができる必要がある。また、クライアントに関連する情報（登録情報、クライアントデータ、又はクライアント課金データ）を、サーバのトラステッド構成要素1106自体の内部に、又はサーバのトラステッド構成要素1106により監視される関連のメモリ内に、セキュアに保持するよう構成される必要がある。この場合にも、課金、報告、及び測定機能をサーバのトラステッド構成要素1106に含めることが望ましい。

【０１０１】

ユーザスマートカード1008は一般に、その使用時に、クライアントのトラステッド構成要素1003、サーバのトラステッド構成要素1106、又はその両者を認証できることを必要とすることになる。ユーザスマートカード1008はまた、サーバのトラステッド構成要素1106のデータ保護機能を検証できることが望ましい。

【０１０２】

イメージ送信コード1103は、クライアントプラットフォームがイメージコード

をセキュアに扱い（好適には該操作はクライアントのトラステッド構成要素の認証を含み、サーバのトラステッド構成要素内で最良に操作されることになる）、及びクライアントプラットフォーム（又はそれに伴うスマートカード）がイメージデータを受信するようライセンス供与その他の態様で許可されているか否かを扱うよう構成されなければならない。イメージ送信コードはまた、クライアントプラットフォームから受信されるイメージデータ（又はデータ実行）に関する要求を受信し解釈するよう構成されなければならない。イメージ送信コードはまた、クライアントプラットフォーム又はユーザスマートカードからユーザアカウント情報を入手する必要がある場合もある。イメージ送信コード1103はまた、クライアントプラットフォームとのセキュアな通信に関与できる必要もある（おそらくはサーバのトラステッド構成要素内の暗号プロセッサの支援を伴うことになる）。

【０１０３】

イメージ受信コード1004は、イメージデータに関する要求を直接的に行い、又はサーバ上で実行するコードに関する要求を行い、及びサーバからイメージデータを受信するために、サーバと通信するよう構成されなければならない。イメージ受信コードは、サーバ、ユーザ、又はクライアントプラットフォームと対話する任意の他者により信頼されることが望ましい。したがって、クライアントプラットフォームのブート後に、クライアントのトラステッド構成要素がイメージ受信コード1004の完全性基準を測定する（及び該完全性基準が格納されている基準と一致しない場合にユーザに警告し又はブートを失敗させる）ことが好ましい。この場合も、イメージ受信コード1004は、サーバとセキュアに通信するために、おそらくは図８に示すタイプのセキュアな通信経路に沿って（おそらくはクライアントのトラステッド構成要素内部の）暗号プロセッサと対話する必要がある。

【０１０４】

基本的な動作原理は、アプリケーションがサーバ1109上で（全体的に又は部分的に）実行されることである。サーバのトラステッド構成要素1106とクライアントのトラステッド構成要素1003と（又はおそらくはスマートカード1008上のユーザのトラステッド構成要素と）の相互の認証が最初に達成されて（実質的に図５

において説明した通り）、アプリケーションを実行することが可能となる。アプリケーションが実行されると、サーバ1109は、クライアントのトラステッド構成要素1003にイメージデータ1108をセキュアに提供し、次いで該イメージデータ1108を使用してディスプレイ1005が駆動される。ユーザデータは有用な動作のために必要とされることになる。該ユーザデータは、クライアントプラットフォームにおけるユーザ入力により（また場合によってはクライアントプラットフォームに格納されているデータから）提供され、再びサーバ1109にセキュアに返送されて（ユーザデータメッセージ1010）、アプリケーションにより使用されることになる。かかる通信は、ディスプレイ1005に対する更新が必要になる度に、又はユーザ入力が必要となる際に、繰り返される。

【０１０５】

本プロセスは、多数の異なる任意の動作モデルに従って動作することが可能である。トラステッドサーバ1109は、ソフトウェア開発者により制御することが可能であり、試用ソフトウェアをユーザに提供する方法として、又はユーザが従量制でソフトウェアを使用することを可能にするために、使用することが可能である。トラステッドサーバのオペレータは、かかる目的のためであっても、ソフトウェア開発者である必要はなく、データを自分のプラットフォーム上で実行する（また代替的には開発者から入手したイメージを中継する）、ソフトウェア開発者により信頼された他人とすることも可能である。更に、トラステッドサーバが、ユーザとソフトウェア開発者の間の媒介として作用することを提供するインターネットサービスプロバイダにより制御されることが考えられる。

【０１０６】

要するに、本構成により、（最も一般的な意味では）「サービスプロバイダ」が、情報を、該サービスプロバイダにより提供された情報が意図されない用途に使用されることが決してない程度のセキュリティを持たせて、ユーザの画面の一部又は全部に提供する（実際には制御する）ことが可能となる。したがって、これは、コンテンツを従量ベースで提供する際に有効な（おそらくは対話形式のコンテンツにとって特に有効な）方法となり得る。サービスプロバイダがディスプレイ1005の事実上の制御を行うため、予約された領域1006は、ユーザではなくサ

ービスプロバイダにより選択された目的（広告、所有権を有する情報、又はその他のユーザが要求したサービス（試用ソフトウェア、コンテンツ提供等）とは直接関係のない情報の表示等）で使用することが可能となる。該サーバにより決定される情報は、（図１０に示すような）既定の領域中に、又は様々な領域に（例えば、所定の時間間隔で、又はコード動作又はユーザにより要求された情報における中断(pause)中に画面全体にわたり）提供することが可能であり、該情報は静的なもの又は時間的に変化するものとすることが可能であり（例えばストリーミングビデオ）、また音声情報を補足することも可能である。

【０１０７】

かかる構成においてサービスを行う際に多数の異なるモデルが使用可能である。最も単純な形態では、「ライセンス供与された」データはクライアント上ではなくサーバ上で実行される。支払いと引き替えに、クライアントは、トラステッドサーバ上でのデータの実行に対応するイメージング情報を受信する。これは、サーバ上のリモートイメージ送信コードを介して送信される。その後、クライアントマシン上のリモートイメージ受信コードは、ユーザの選択に対応するキーボードストロークをサーバに送信し、折り返しアプリケーションの実行の変化に対応するイメージング情報を受信する。該イメージング情報は、トラステッドサーバからＰＰＴＰ等のセキュアなチャネルを介してクライアント内のトラステッド構成要素に直接送信され、該構成要素は、コンピューティング装置の信頼できない部品を全く伴わずに直接イメージング情報を表示するよう構成される。

【０１０８】

全てのソフトウェアをクライアントではなくサーバ上で実行することは、全ての場合に効率的なものとはならない。比較的機密性の高い情報の場合には（これは、データアクセス、又はソフトウェアが実行する度に実質的な重複が存在するおそれがある場合に該当する）、全てのイメージをクライアントの保護されたメモリに一時的に格納し、ソフトウェアをクライアント上に表示させるが、実際にはサーバ上で実行しているようにするのが適当である。クライアントは、保護されたメモリに格納されているイメージとは別にソフトウェアを格納する段階がないため、ハードディスク又は他の格納媒体を介したデータのライセンス侵害攻撃

を受ける余地がない。より機密性の低い情報の場合には、特に、通常ゲームソフトウェアの場合のように動作の度にアプリケーションが異なるイメージを生成し得る場合には、おそらくはソフトウェアを部分的にサーバから実行する方が適当であり、例えば、実質的にはローカルで実行するが、当該ソフトウェアを実行するためにサーバからの所定の重要な入力（オンラインサービス等）が必要となる。サーバは依然として全体的な制御を行う必要があり、このため、クライアントマシンがプログラムを実行する能力を有していても、サーバの関与なしに該実行が成功することはない。これを達成するための様々な方法が存在し、例えば、サーバが、情報のキービットを供給し、全てのクライアントにとって同一となる共同(communal)ブロックでイメージを送信し、クライアントのトラステッド構成要素がサーバのトラステッド構成要素に対して個人情報又はキービットの認証を繰り返し行うことが可能であり、又は、データの一部をローカルに格納し、サーバが更なるデータを保護されたメモリに送信することが可能である。効率化のため、実行中又は実行後に、保護されたメモリに情報の一部（キービット等）のみを格納し、残りをハードディスクその他の格納媒体に格納することが可能である。このイメージ転送を行う部分的なモデルは、同一サーバ上の異なるデータに関する全体のモデルと同時に使用することが可能である。

【０１０９】

次いで、クライアントのトラステッドプラットフォーム1001がトラステッドサーバ1109からのイメージデータの表示を行う「トラステッド端末」として働くように図１０の構成を動作させる手順について図１１を参照して説明する。本構成は、上述の「サービス」の何れについても有用なものとなり、例えば、クライアントのトラステッドプラットフォーム1001のユーザが文書を見たい（が取得しない）場合、又はペイ・パー・ユーズ・ベースでソフトウェアを使用したい場合に有用なものとなる。

【０１１０】

図１１に示す構成において、ユーザスマートカード1008は、サーバ1109とのユーザ対話を提供するために使用され、クライアントのトラステッド構成要素1003は、クライアント1001が信頼できる表示を提供できることを確認するよう機能す

ると共に、ユーザスマートカード1008とクライアントのトラステッド構成要素1003との間の媒介として作用する。代替的な構成では、クライアントのトラステッド構成要素1003は、ユーザスマートカード1008のためでなくユーザのために動作することが可能であり、この場合には、ユーザスマートカード1008とサーバ1109（通常はサーバのトラステッド構成要素1106）との対話は、クライアントのトラステッド構成要素1003とサーバ1109との対話に置き換えることが可能である。

【０１１１】

クライアントのトラステッドプラットフォーム1001の「トラステッド端末」動作を機能させるための初期設定からなる第１の段階は、トラステッド端末機能が要求された時点又はそれよりも早期に発生することができる。トラステッドサーバ1109とユーザスマートカード1008との間で対話がなされる場合には、初期設定段階は、クライアントのトラステッドプラットフォーム1001を使用する必要が全くなく、すなわち、他のクライアントのトラステッドプラットフォームを使用することが可能である（この場合には、スマートカードに登録する利点は、実質的に任意のクライアントのトラステッドプラットフォームをトラステッド表示機能と共に使用して該スマートカードが登録されたデータ又は動作にアクセスできることである）。代替的には、全ての設定ステップを、トラステッドサーバ1109上の特定のデータ又は動作についてトラステッド端末の実行を可能にするよう構成された特定のスマートカード1008の発行と置き換えることが可能である（これは、ユーザの主たるスマートカードに対する補助として使用されるスマートカードとすることが可能であり、これを実行する構成については、「Computing Apparatus and Method of Operating Computing Apparatus」と題する、2000年3月3日付けで出願された本出願人の同時係属中の国際特許出願第PCT/GB00/00751号に記載されている）。

【０１１２】

第１の段階の開始時に、ユーザは、自分のスマートカード1008（又は上述のクライアントプラットフォーム1001…スマートカードの登録ではなくクライアントプラットフォームの登録については以下では明示的には説明しないこととする）をトラステッドサーバ1109に登録する（ステップ1100）。この段階で支払い機構

を構成することが可能である。単純なアプローチ（ステップ1105）として、所定量のデータ購入又はコード使用をカバーするようにスマートカード1008にクレジットで請求することが挙げられるが、他のモデル（スマートカード、クライアントプラットフォーム、トラステッドサーバ、又はその他の場所による又はそれに対する請求の詳細の提供及びセキュアなログを行う機構の確立及び使用データの報告等）も可能である。登録ステップ1100で既に受信されていない場合には、スマートカード1008は、今度はその公開鍵をトラステッドサーバ1109に提供する（ステップ1110）。折り返し、トラステッドサーバ1109は、サーバのトラステッド構成要素1106の公開鍵証明書をユーザスマートカード1008にインストールする（ステップ1115）。これにより、該スマートカード1008によるトラステッドサーバ1109の認証が可能になり、すなわち、ナンスを含むユーザスマートカード1008による認証要求に応じて、トラステッドサーバ1109が、その公開鍵証明書及びナンスを含みその秘密鍵で署名したメッセージを返送し、こうして、ユーザスマートカードは、メッセージが真にトラステッドサーバ1109から発信されたことを確認することができる。好ましくは（ステップ1120）、ユーザは、ユーザスマートカード1008を使用してサーバのトラステッド構成要素1106の保護能力を（サーバのトラステッド構成要素1106により又はこれを参照して保持され又は入手することができる完全性基準その他の信頼できるデータから）検証して、トラステッドサーバが実際に信頼できることを確認する。

【０１１３】

第２の段階は、データ実行であり、トラステッドディスプレイを有するクライアントプラットフォームの使用を必要とする。第１のステップは、トラステッドサーバ1109からのみ入手可能なデータを表示するための（通常はクライアントのトラステッドプラットフォーム1001のオペレーティングシステムを介した）要求である（ステップ1125）。スマートカードモデルの場合には、ユーザスマートカード1008は、クライアントのトラステッドプラットフォーム1001とセッション中である必要がある。次のステップ（ステップ1130）は、存在する異なるトラステッド構成要素（すなわち、図１１に示す構成の場合、ユーザスマートカード1008、クライアントのトラステッド構成要素1003、及びサーバのトラステッド構成要

素1106）の間の相互認証の１つである。随意選択的に、ユーザスマートカード1008とクライアントのトラステッド構成要素1003との間の認証の場合に、この時点でユーザスマートカード1008に固有の特殊な表示メッセージ（印章イメージ）をディスプレイ1005に表示して（このプロセスについては「System for Digitally Signing a Document」と題する2000年5月25日付けで出願された本出願人の同時係属中の国際特許出願第PCT/GB00/012296号により詳細に記載されている）、本プロセスを続行したい旨の確認（及びおそらく例えばパスワードを入力することによるスマートカードと本人の関連性の更なる認証）を与えるようユーザに要求し、この場合には、ユーザスマートカード1008をスマートカードリーダ1107に残すことができる。

【０１１４】

次いで、クライアントプラットフォーム1001のオペレーティングシステムにより要求されるイメージデータが、トラステッドサーバ1109により、好ましくはセキュアな通信チャネル又はプロセス（ＰＰＴＰといった）により、保護されたメモリ1009に提供される（ステップ1140）。随意選択的に、イメージ転送ログが作成又は更新される（ステップ1145）。イメージ転送ログの作成及び維持に対する代替的なアプローチについては更に後述する。別の随意選択的なステップ（ステップ1150）は、イメージデータの署名をサーバのトラステッド構成要素の公開鍵によりチェックし、このデータが実際に期待される発信源からのものであるかを検証することにより、ユーザスマートカード1008により完全性チェックを実行することである。

【０１１５】

次いで、トラステッドサーバ1109から受信されたイメージデータが、クライアントのトラステッド構成要素1003のトラステッド表示プロセッサ機能の制御下で動作するディスプレイ1005に表示される（ステップ1155）。表示されたイメージの少なくとも一部は保護されたメモリ1009に格納されたものであり、表示されたイメージの他の部分は、適当な構成においてクライアントプラットフォーム1001において完全に動作するプロセスからのものとすることが可能である。次いで、ユーザは、入力を通常のユーザインタフェイスを介してクライアントのトラステ

ッドプラットフォーム1001に提供し、該情報は、この場合も好ましくはセキュアな通信チャネルを使用してトラステッドサーバ1109に（メッセージ1010として）提供される（ステップ1160）。次いで、ユーザ選択に従って、トラステッドサーバ1109上でのデータの実行が修正され、又は代替的なデータが選択され、その結果として、修正されたイメージデータがトラステッドサーバ1109により提供される（ステップ1165）。次いでステップ1145～1165のプロセスを必要な頻度で繰り返すことが可能である。本セッションを終了する要求（例えばクレジットを使い果たした場合）は、トラステッドサーバ1109又はユーザによりなされる（ステップ1170）。随意選択的に、この後に、使用ログの作成又は更新を行うことが可能であり（かかるログの代替策の可能性については後述する）、これに加えて又は代替的にユーザに請求を行うことが可能である（ステップ1175）。

【０１１６】

イメージデータの提供が無料又は無制限である場合（例えば、トラステッド端末構成を使用する目的が個々のユーザに対する実行コードの開放を防止することのみである場合、又は要求される唯一の「支払い」がトラステッドサーバにより提供される広告である場合）には、使用ログ（又は課金情報）を提供する必要がない場合もある。使用ログが必要である場合には、これを提供するために使用可能な選択肢が少なくとも３つ存在する。

【０１１７】

第１の選択肢は、使用情報をトラステッドサーバ1109に格納することである。クライアントプラットフォーム1001に対するイメージデータ転送の度にトラステッドサーバ1109により使用ログを採取することができる。課金情報（クレジットカードその他の使用を課金できる口座等）は、登録プロセスにおいてユーザから（スマートカード若しくはクライアントのトラステッド構成要素により又は他の場所から）取得することが可能であり、またトラステッドサーバ1109に格納することができる。好適には、かかる情報の全て（特にユーザ口座情報）がサーバのトラステッド構成要素1106内に保持される。代替的には、情報をトラステッドサーバ1109内の他のメモリに保持し、サーバのトラステッド構成要素1106内に保持されている暗号鍵によりセキュアに保管することである。

【０１１８】

第２の選択肢は、使用情報をクライアントのトラステッドプラットフォーム1001に、好ましくはクライアントのトラステッド構成要素1003内に格納する（また代替的には、保護されたメモリ1009内に保持し、又はクライアントのトラステッド構成要素1003内に保持されている暗号鍵によりセキュアにしてクライアントのトラステッドプラットフォーム1001内の保護されたメモリ1009若しくはその他のメモリ内に保管する）ことである。次いでトラステッドサーバ1109（好ましくは、サーバのトラステッド構成要素1106）は、必要に応じてクライアントのトラステッドプラットフォーム1001に問い合わせをして使用情報を見つけ出し、代替的には、クライアントのトラステッドプラットフォーム1001が使用情報をトラステッドサーバ1109に所定の時間又は間隔で報告することが可能である。これに対する１つのアプローチとして、トラステッドサーバ1109がクライアントのトラステッドプラットフォーム1001にアプレットをダウンロードして使用又は課金情報の報告を行わせること、又はどのイメージデータが既にユーザにより表示されたかをトラステッドサーバ1109が判定することを可能にすることである。トラステッドサーバ1109は、クリアリングハウスとして作用することが可能であり、この場合には、課金に関する情報は、ダウンロードされたソフトウェアを介してクライアントのトラステッドプラットフォーム1106に返送される。この場合も、支払いは、ユーザのクレジットカードの詳細情報をトラステッドサーバ1109に提供することにより行われるのが適当であり、該詳細情報を、クライアントのトラステッド構成要素1003内に保持し（又はクライアントのトラステッド構成要素1003を介してユーザスマートカード1008により提供し）、及びトラステッドサーバ1109に使用情報と共に転送することができる。

【０１１９】

第３の選択肢は、使用情報をユーザスマートカード1008に格納することである。これは、特定のトラステッドプラットフォームではなく特定のユーザによる使用を測定するという利点を有するものであり、特にホットデスキング環境（又は図書館又は空港のラウンジの場合のように公共利用可能なトラステッドプラットフォームが提供された環境）に特に適したものとなり得る。この場合も、トラス

テッドサーバ1109は、（クライアントのトラステッドプラットフォーム1001を介して）スマートカード1008に問い合わせして使用又は口座情報を見つけ出すことが可能であり、又は該情報を、上記第２の選択肢に関して説明したように、おそらくはスマートカード1008にアプレットをダウンロードすることにより、一定の時間又は間隔でトラステッドサーバ1109に提供することが可能である。

【０１２０】

上述のように、データ使用は、勘定をつけるため並びにユーザがアクセスしたデータをチェックするために重要なものとなる場合がある。これが関係する１つの状況として、ユーザが、データに対する特定の数のアクセスを許可される場合（固定使用(fixed usage)ライセンシングモデル等―トラステッドコンピューティングプラットフォームにおいて全て又は一部が実行されるデータの使用に適したライセンシングモデルについては、「Computer Platform and Their Methods of Operation」と題する2000年8月11日付けで出願された本出願人の同時係属中の国際特許出願第PCT/GB00/03101号に更に記載されている）、又は購入前の試用のための限定されたアクセスのみが許可される場合が挙げられる。かかる構成では、トラステッドサーバ1109が、関連するユーザ又はクライアントプラットフォームに関するログファイルを（それが何処に格納されていようと）チェックして、許可された使用を超過していないこと又は決して超過しないことを確実にすることが必要となる可能性がある。使用が超過しているというログからの証拠が存在する（おそらくは当該ソフトウェアを過去に試用している）場合には、トラステッドサーバ1109は、エラーメッセージを生成してクライアントのトラステッドプラットフォーム1001上で（おそらくは（例えばソフトウェアの多数回の試用が許可されないことを示す）ディスプレイ1005により）ユーザに提供し、関連するコードはトラステッドサーバ1109上では決して実行されない（但しこれが適当な場合）。このアプローチにより、開発者は、非認可使用というリスクを伴うことなく、試用ソフトウェアの完全な機能を該ソフトウェアの試用時にユーザに提供することが可能となる。

【０１２１】

かかる構成において、試用ソフトウェアは、例えば、開発者により設定された

制限された回数だけトラステッドサーバ1109上で利用可能となるように提供することが可能となる。上述のクライアント／サーバ構成のトラステッド端末機能を使用することにより、（クライアントを操作している）ユーザが、ソフトウェアをコピーすること、割り当てられた期間より長期間にわたり使用すること、又は該ソフトウェアがライセンスされた契約の他のあらゆる条項に違反できないようにすることが確実となる。この構成は、ソフトウェアの試用に関して特に有効なものであるが、開発者がオブジェクトコードをユーザに提供したくはないがそのコードをユーザに提供してペイ・パー・ユーズのサービスとしてアクセスさせたい場合にも、実施可能な使用モデルを提供するものとなる、ということが理解されよう。

【０１２２】

別の考え得るモデルは、多数の試用の後に試用ライセンスを完全ライセンスに変更することである。この場合には、ユーザがライセンス契約に署名する際に、該ユーザのスマートカード（又はクライアントのトラステッド構成要素）にログファイル（好ましくはセキュアに保持されたログファイル）が設けられることになることが同意される。該ログファイルは、試用ソフトウェアがダウンロードされたこと、該試用ソフトウェアがその使用時に適当なあらゆる機構によりアップデートすることが可能であると共に必要に応じてトラステッドサーバ1109によりアクセスできるものであることを示すものである。例えば、イメージデータをクライアントに送信する前にログファイルをチェックして、その試用が以前に使用されたか又はどの程度の頻度で使用されたかを確認することができ、試用を続行するか否かをサーバが判断し、イメージデータを送信した場合にはログファイルを更新する。所定の時間又は使用回数の後、ソフトウェアの継続的な使用のための支払いを行うことをユーザに促し、又は、所定の使用回数を超過した場合に支払いを行うことを試用契約の一部として同意させることが可能である（この場合には、所定の使用回数を超過した時点で、又はそれよりも早期に、トラステッドサーバ1109に口座情報が提供される）。

【０１２３】

上記から分かるように、本発明による構成は、ソフトウェア開発者又はコンテ

ンツプロバイダが、その製品の経済的価値の損失というリスクを負うことなく、ソフトウェアを完全な機能を持たせて試用させ、又はメータリングベースで提供し、又はコンテンツを試用又はメータリングベースで提供し、又は広告コンテンツを付随させることが可能となるといった大きな価値を提供することができる。

【図面の簡単な説明】

【図１】

本発明の実施形態のうちトラステッドクライアントプラットフォームとしての使用に適したホストコンピュータの構成要素を示す説明図である。

【図２】

図１のホストコンピュータのハードウェアアーキテクチャを示すブロック図である。

【図３】

本発明の実施形態での使用に適したトラステッドデバイスの構成要素を示すブロック図である。

【図４】

完全性基準を得るための好適なプロセスを示すフローチャートである。

【図５】

トラステッドプラットフォームの完全性を検証するプロセスを示すフローチャートである。

【図６】

スマートカードを用いたユーザによるトラステッドプラットフォームの完全性の検証プロセスを示すフローチャートである。

【図７】

図６のプロセスでの使用に適したユーザスマートカードの処理エンジンを示すブロック図である。

【図８】

トラステッドデバイスとホストコンピュータの他の構成要素との間のトラステッド通信経路を提供するための図２の構成の変形例を示すブロック図である。

【図９】

暗号機能を有するホストコンピュータの唯一の構成要素がトラステッドデバイスである場合に図８の構成において到来するメッセージを復号するプロセスを示すブロック図である。

【図１０】

本発明の一実施形態によるクライアント／サーバシステムの基本的な構成要素を示すブロック図である。

【図１１】

本発明の一実施形態による図１０のクライアント／サーバシステムのトラステッド端末動作のためのプロセスを示す説明図である。

【符号の説明】

1001　クライアント

1002　セキュアな通信経路

1004　メモリ（リモートイメージ受信コード）

1005　ディスプレイ

1006　サーバにより制御される選択領域の画素

1007　カードリーダ

1008　スマートカード

1009　保護されたメモリ

1010　ユーザデータ

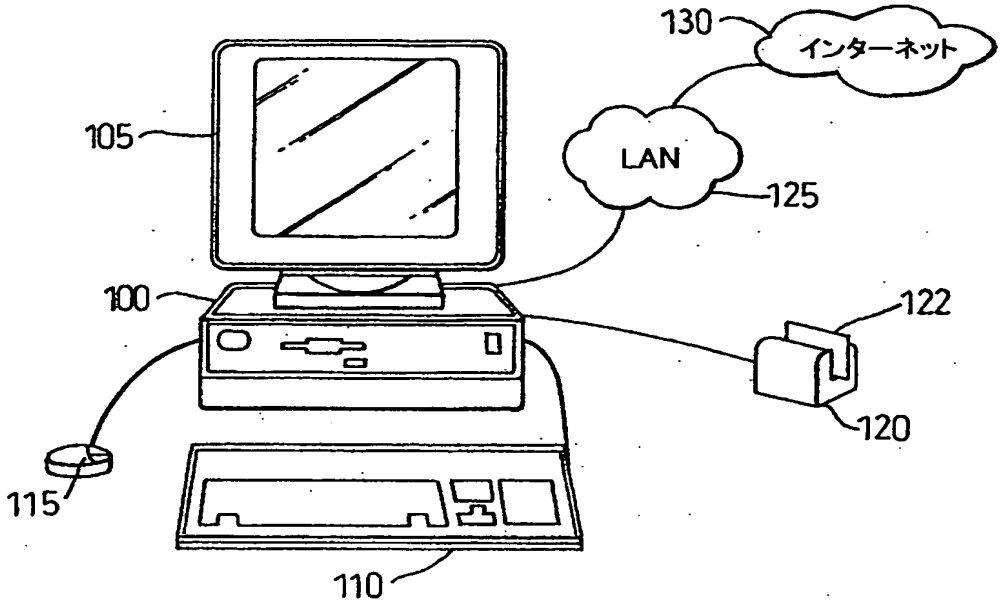
1103　メモリ（リモートイメージ送信コード）

1107　データ／コード

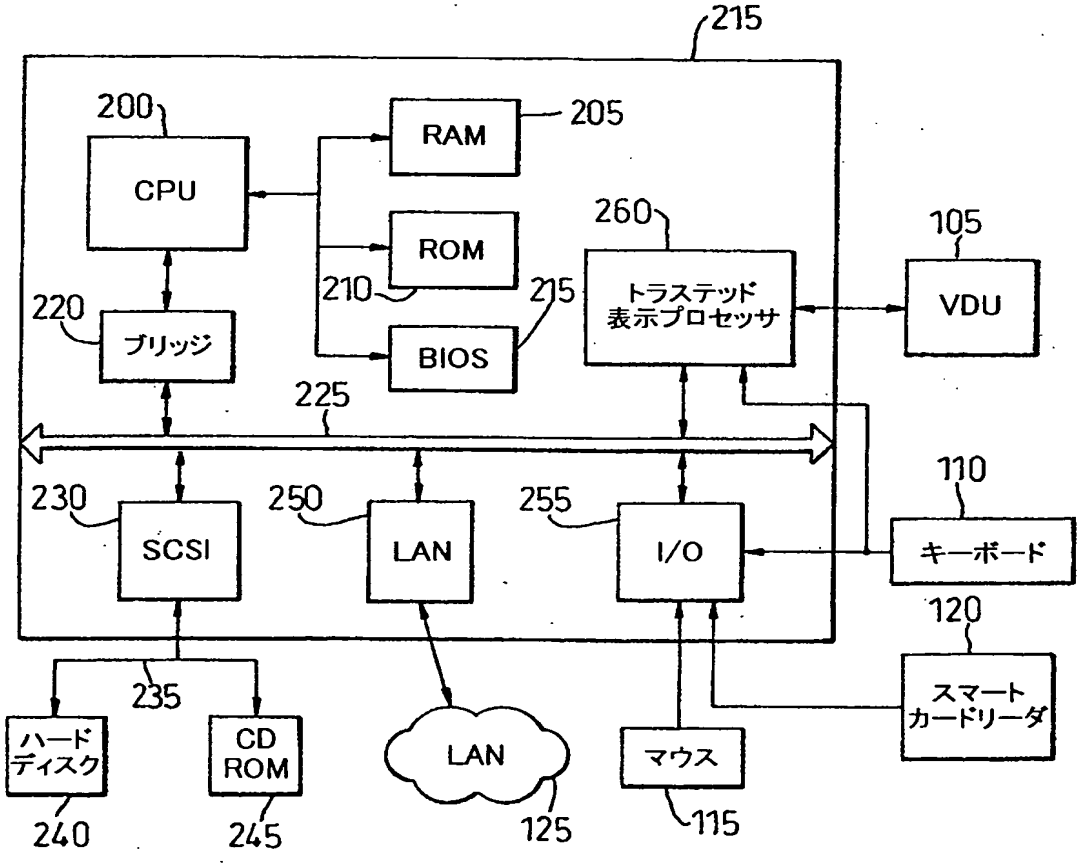
1108　イメージデータ

1109　サーバ

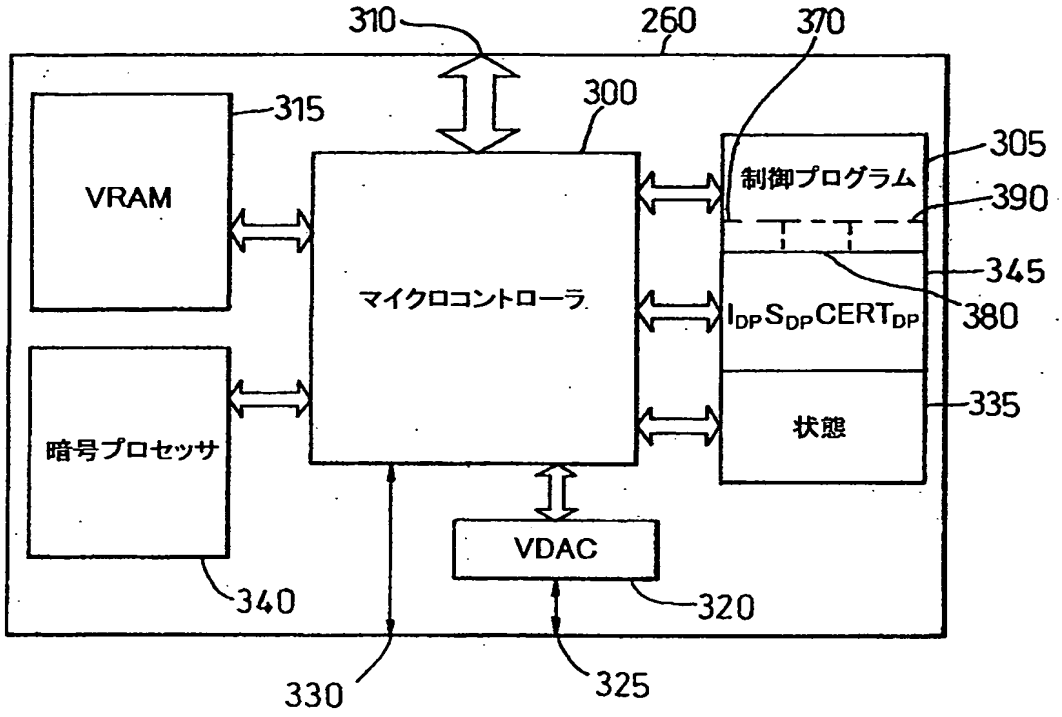
【図１】


130
インターネット
105
LAN
125
100
122
120
115
110

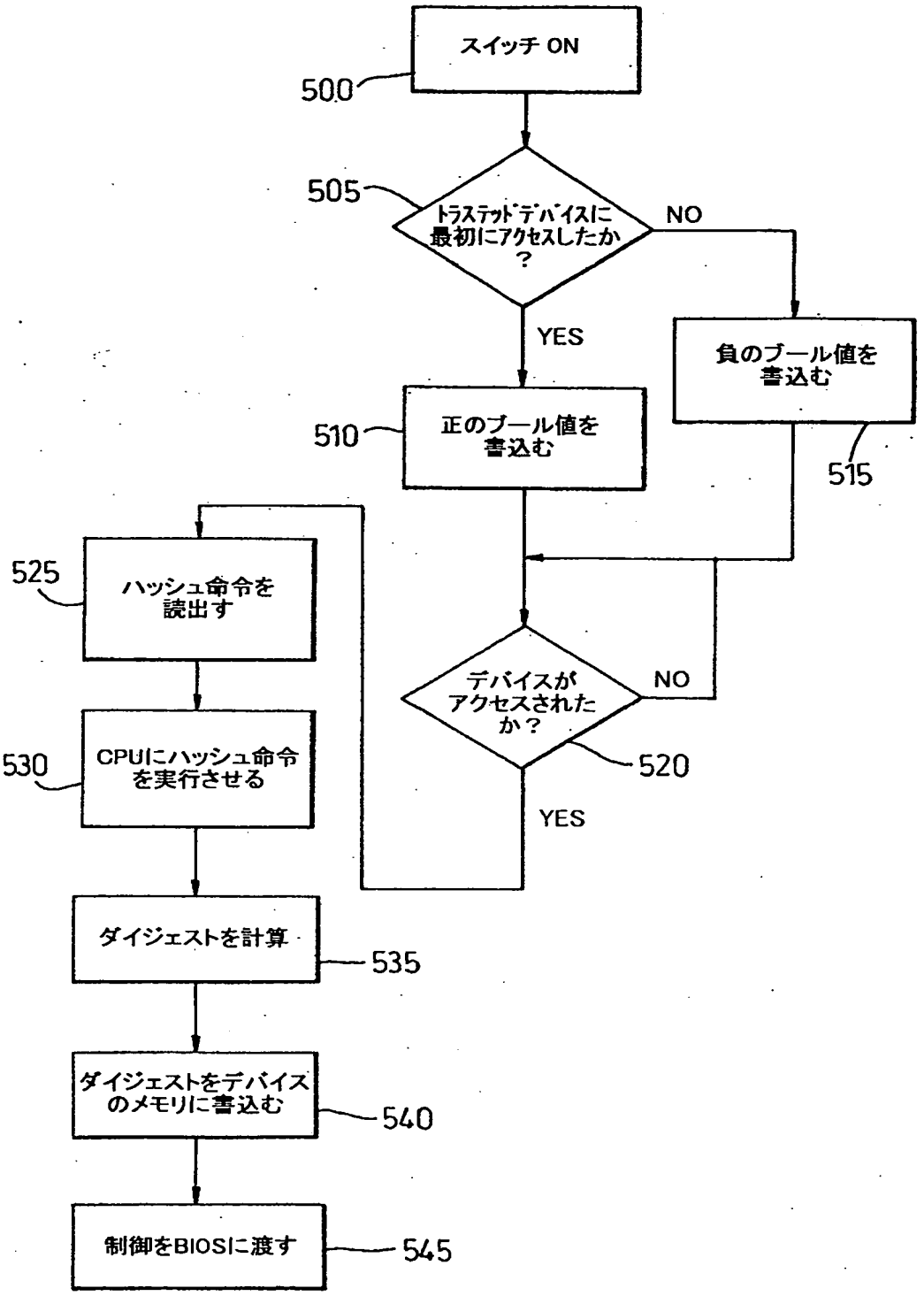
【図２】


215
200
CPU
RAM
205
ROM
210
BIOS
215
260
トラステッド
表示プロセッサ
105
VDU
220
ブリッジ
225
230
SCSI
250
LAN
255
I/O
110
キーボード
120
スマート
カードリーダ
235
ハード
ディスク
240
CD
ROM
245
LAN
125
マウス
115

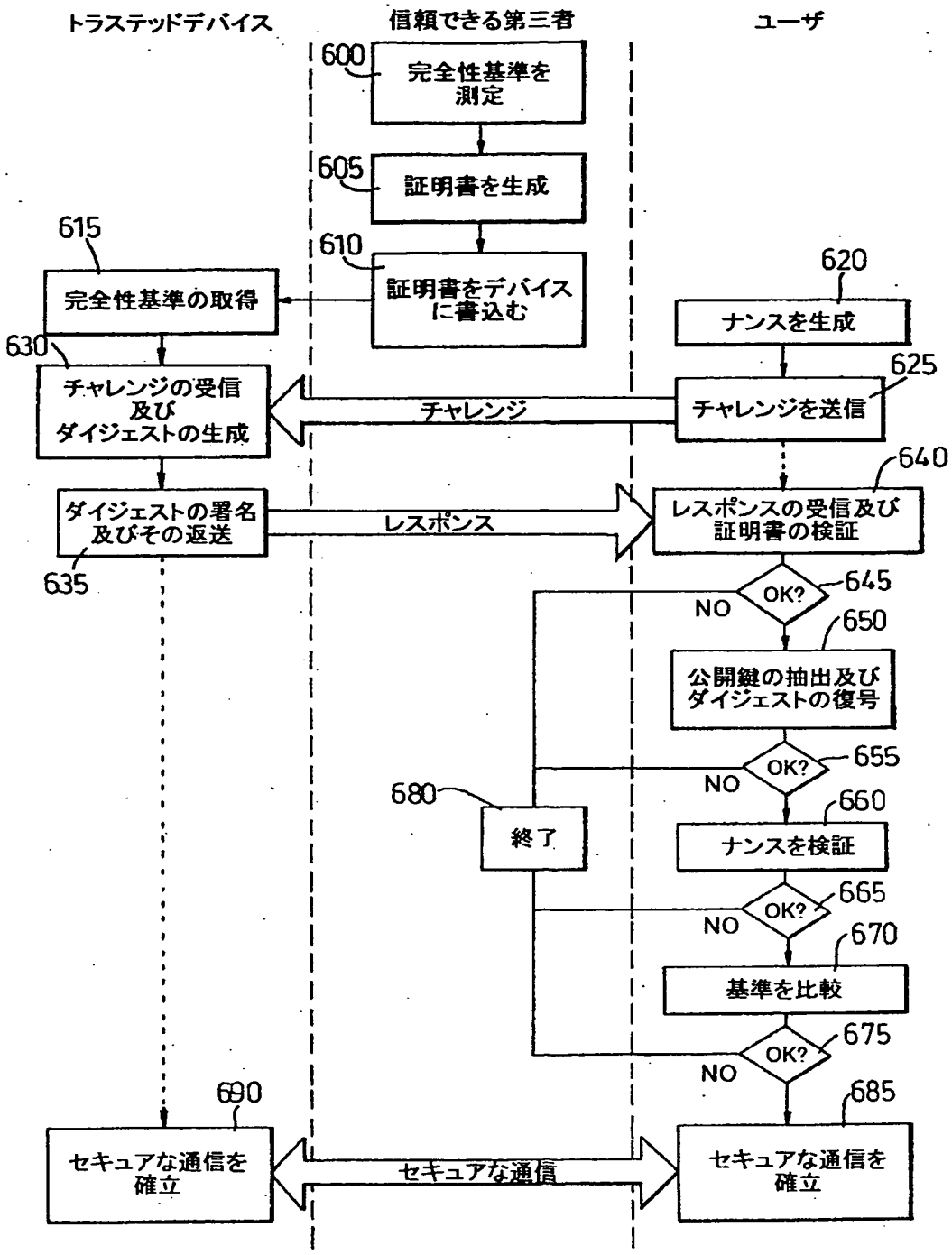
【図３】


310
260
370
315
300
305
VRAM
制御プログラム
390
345
マイクロコントローラ
$I_{DP}S_{DP}CERT_{DP}$
380
335
暗号プロセッサ
状態
VDAC
340
320
330
325

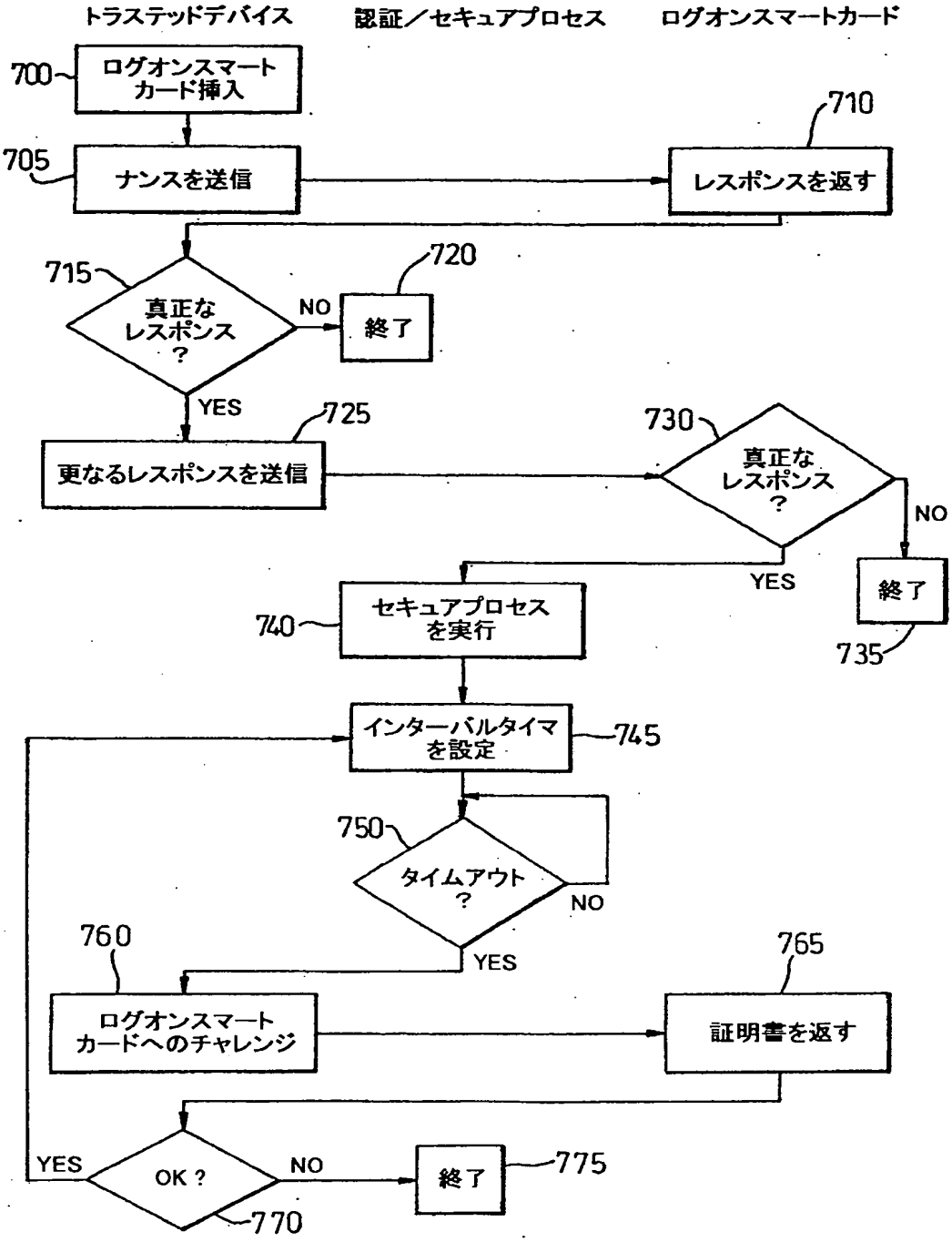
【図４】


スイッチ ON
500
505
トラステッドデバイスに最初にアクセスしたか？
NO
YES
負のブール値を書込む
515
510
正のブール値を書込む
525
ハッシュ命令を読出す
デバイスがアクセスされたか？
NO
520
530
CPUにハッシュ命令を実行させる
YES
ダイジェストを計算
535
ダイジェストをデバイスのメモリに書込む
540
制御をBIOSに渡す
545

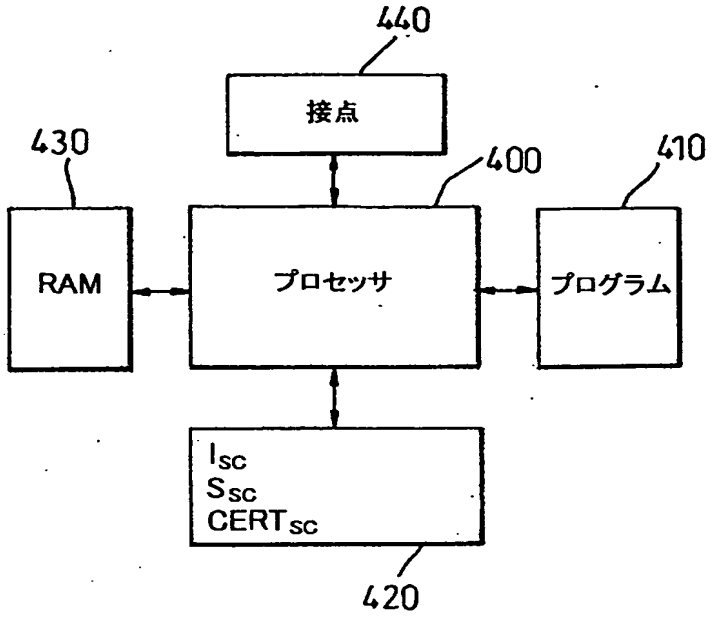
【図５】


トラステッドデバイス
信頼できる第三者
ユーザ
600
完全性基準を測定
605
証明書を生成
610
証明書をデバイスに書込む
615
完全性基準の取得
620
ナンスを生成
630
チャレンジの受信及びダイジェストの生成
チャレンジ
625
チャレンジを送信
640
ダイジェストの署名及びその返送
635
レスポンス
レスポンスの受信及び証明書の検証
OK?
645
NO
650
公開鍵の抽出及びダイジェストの復号
OK?
655
NO
680
終了
660
ナンスを検証
OK?
665
NO
670
基準を比較
OK?
675
NO
690
685
セキュアな通信を確立
セキュアな通信
セキュアな通信を確立

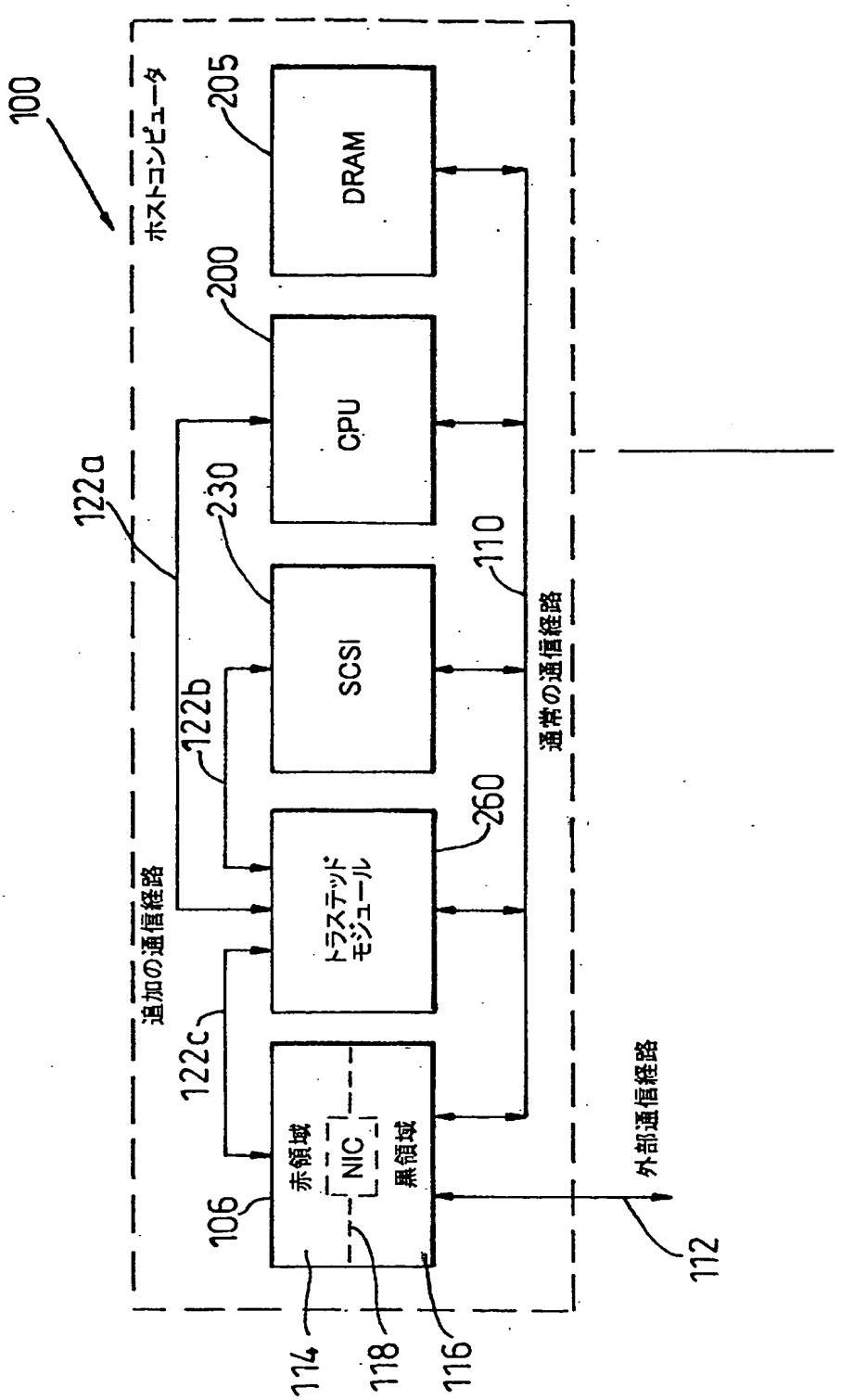
【図６】


トラステッドデバイス
認証／セキュアプロセス
ログオンスマートカード
700
ログオンスマートカード挿入
705
ナンスを送信
710
レスポンスを返す
715
真正なレスポンス？
NO
720
終了
YES
725
更なるレスポンスを送信
730
真正なレスポンス？
NO
終了
735
YES
740
セキュアプロセスを実行
インターバルタイマを設定
745
750
タイムアウト？
NO
YES
760
ログオンスマートカードへのチャレンジ
765
証明書を返す
YES
OK？
NO
終了
775
770

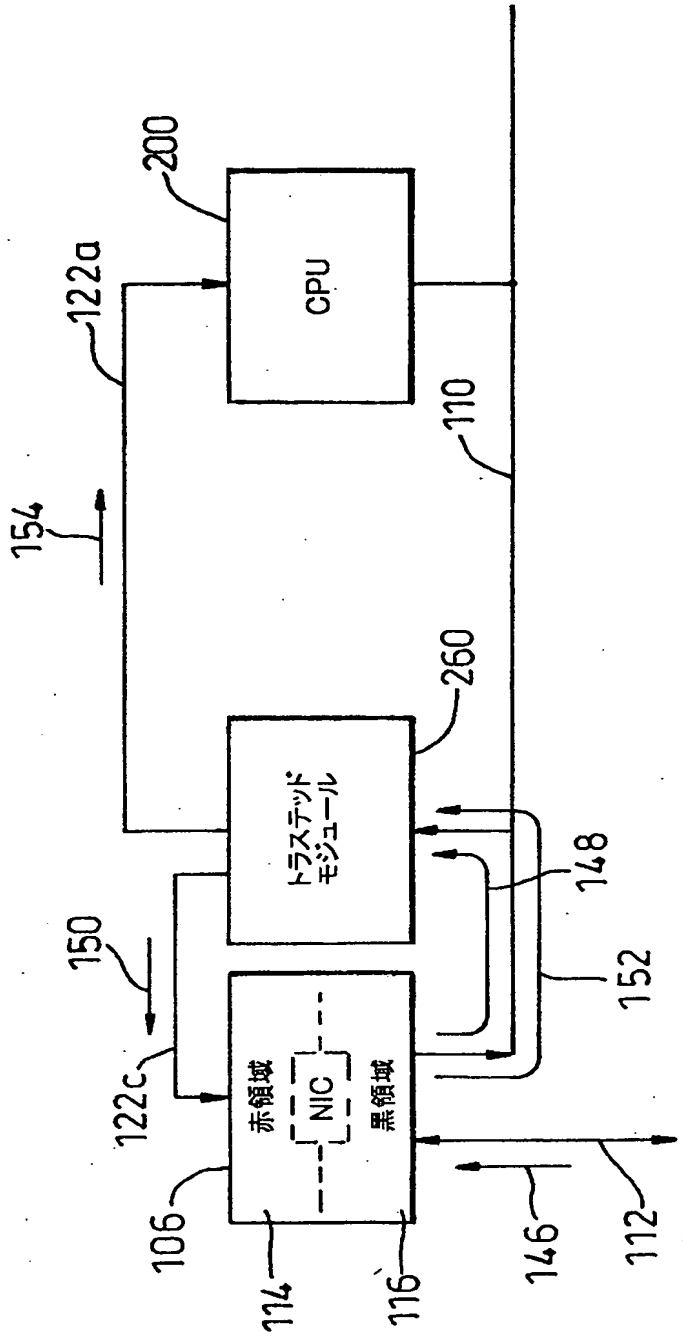
【図７】



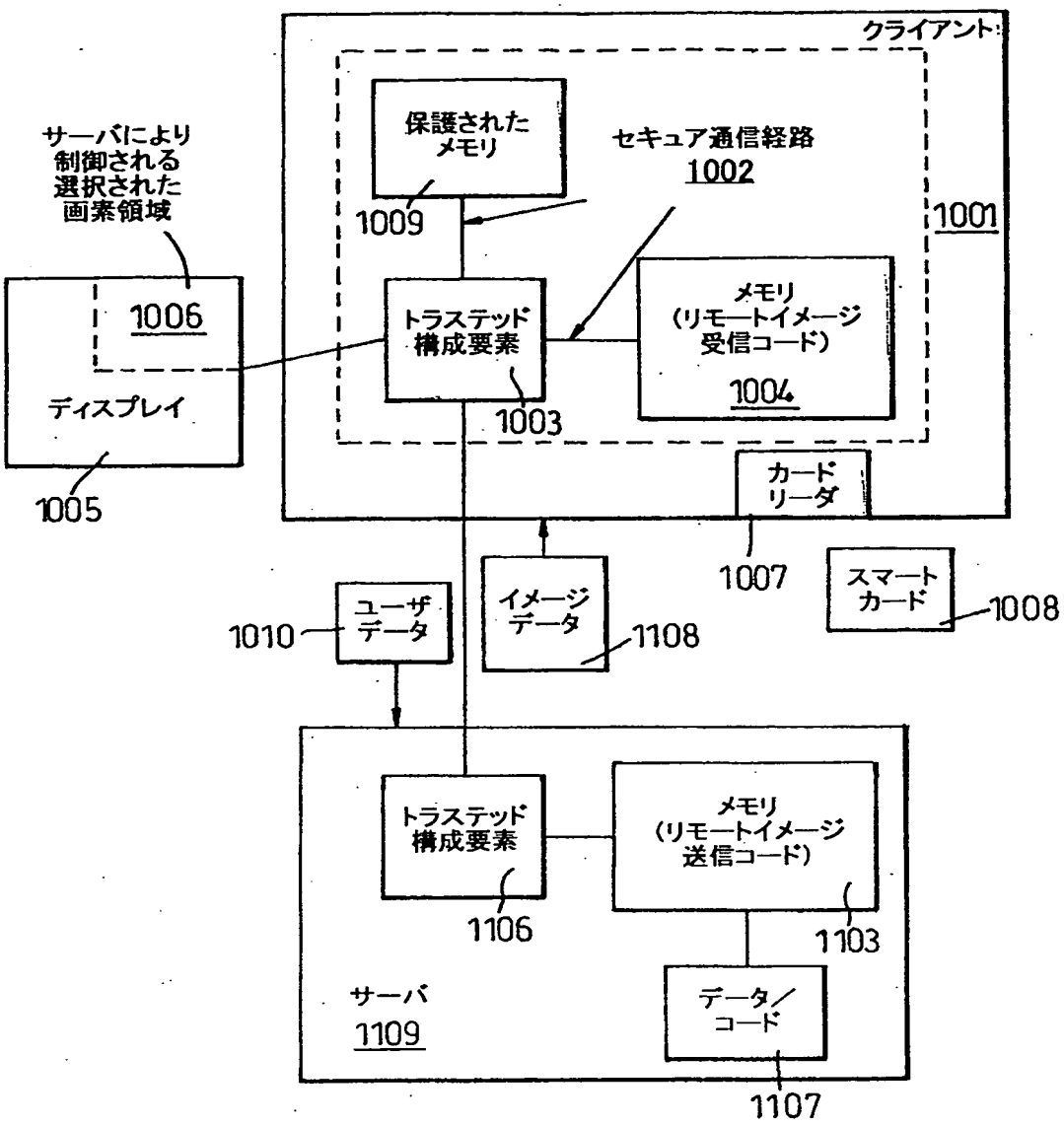
【図８】


100
ホストコンピュータ
205
DRAM
200
CPU
230
SCSI
110
通常の通信経路
122a
122b
122c
追加の通信経路
260
トラステッド
モジュール
赤領域
NIC
黒領域
106
外部通信経路
112
114
118
116

【図９】

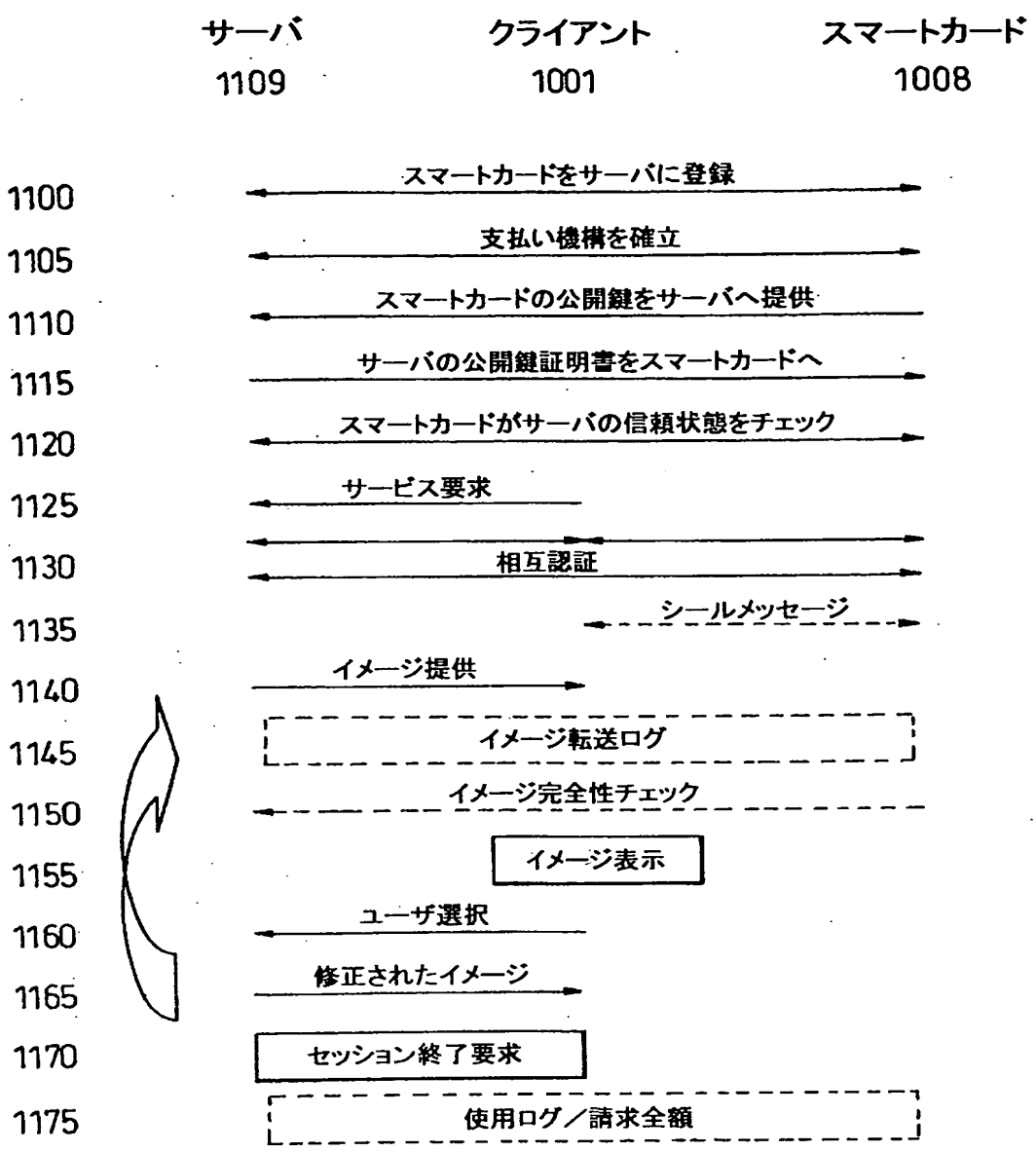

200
CPU
122a
110
154
260
トラステッド
モジュール
148
150
152
122c
赤領域
NIC
黒領域
106
114
116
146
112

【図１０】



イメージ伝送システムの論理図

【図１１】


サーバ
1109
クライアント
1001
スマートカード
1008
1100
スマートカードをサーバに登録
1105
支払い機構を確立
1110
スマートカードの公開鍵をサーバへ提供
1115
サーバの公開鍵証明書をスマートカードへ
1120
スマートカードがサーバの信頼状態をチェック
1125
サービス要求
1130
相互認証
1135
シールメッセージ
1140
イメージ提供
1145
イメージ転送ログ
1150
イメージ完全性チェック
1155
イメージ表示
1160
ユーザ選択
1165
修正されたイメージ
1170
セッション終了要求
1175
使用ログ／請求全額

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Intern nal Application No
PCT/GB 00/03689

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 44402 A (BRAMHILL IAN DUNCAN ;SIMS MATTHEW ROBERT CHARLES (GB); BRITISH TEL) 8 October 1998 (1998-10-08) abstract; figure 4 page 1, line 1 -page 3, line 9 page 7, line 6 -page 8, line 25	18-20, 22-24
Y	page 14, line 27 -page 15, line 6 page 18, line 20 - line 25	1-5, 9-11, 14-17,21
A	--- -/—	6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 January 2001	09/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/GB 00/03689

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,Y	US 6 006 332 A (CHRISTIAN BRIAN S ET AL) 21 December 1999 (1999-12-21) abstract; figure 2 column 10, line 49 -column 11, line 8 column 13, line 14 - line 45 column 20, line 19 - line 43	1,9-11, 14-17,21
P,A	---	4,13
Y	US 5 933 498 A (ABRAMS MARSHALL D ET AL) 3 August 1999 (1999-08-03) the whole document	2-5

A	US 5 473 692 A (DAVIS DEREK L) 5 December 1995 (1995-12-05)	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter　nal Application No
PCT/GB 00/03689

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9844402 A	08-10-1998	AU 6414098 A	22-10-1998
		EP 0970411 A	12-01-2000
US 6006332 A	21-12-1999	NONE	
US 5933498 A	03-08-1999	AU 1690597 A	01-08-1997
		CA 2242596 A	17-07-1997
		EP 0880840 A	02-12-1998
		JP 2000503154 T	14-03-2000
		WO 9725798 A	17-07-1997
US 5473692 A	05-12-1995	AU 3583295 A	27-03-1996
		EP 0780039 A	25-06-1997
		JP 10507324 T	14-07-1998
		WO 9608092 A	14-03-1996
		US 5568552 A	22-10-1996

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
Ｈ０４Ｎ	5/91	Ｈ０４Ｎ	7/16	Ｚ
	7/16	Ｇ０６Ｆ	9/06	６６０Ａ
		Ｈ０４Ｎ	5/91	Ｐ

(72)発明者　チェン，リクン
イギリス国ブリストル・ビーエス32・９ディーキュー，ブラッドレイ・ストーク，ハーベスト・クローズ・１

Ｆターム(参考)　5B058 CA01 CA27 KA31 KA35 YA20
5B076 FA13 FB05 FB16
5B085 AC04 AE04 AE12 BA06 BG02
BG07
5C053 FA13 LA15
5C064 BA01 BB01 BB02 BC06 CA14